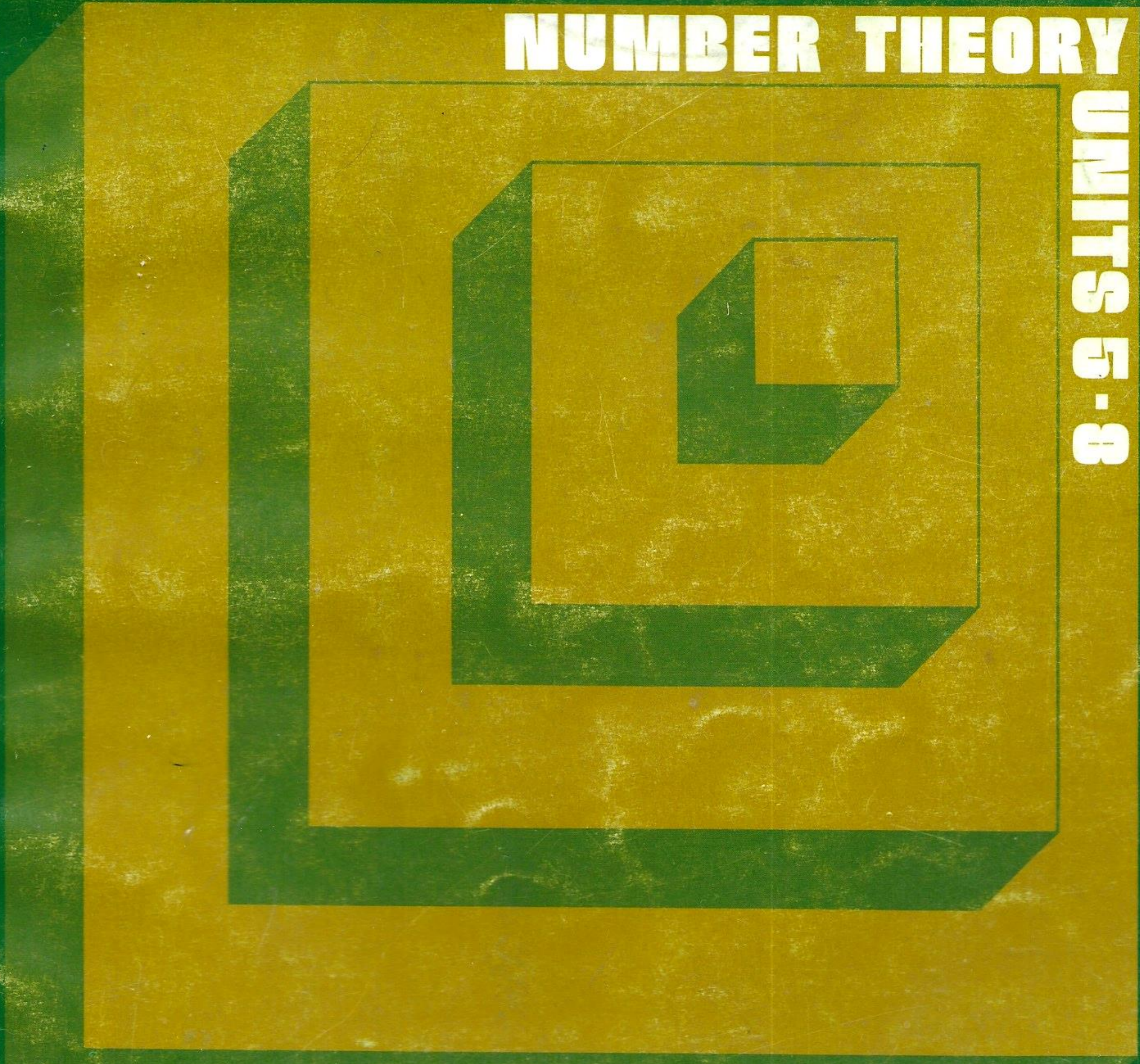
M335 NT 5-8

THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics

STUDIES IN PURE MATHEMATICS

NUMBER THEORY

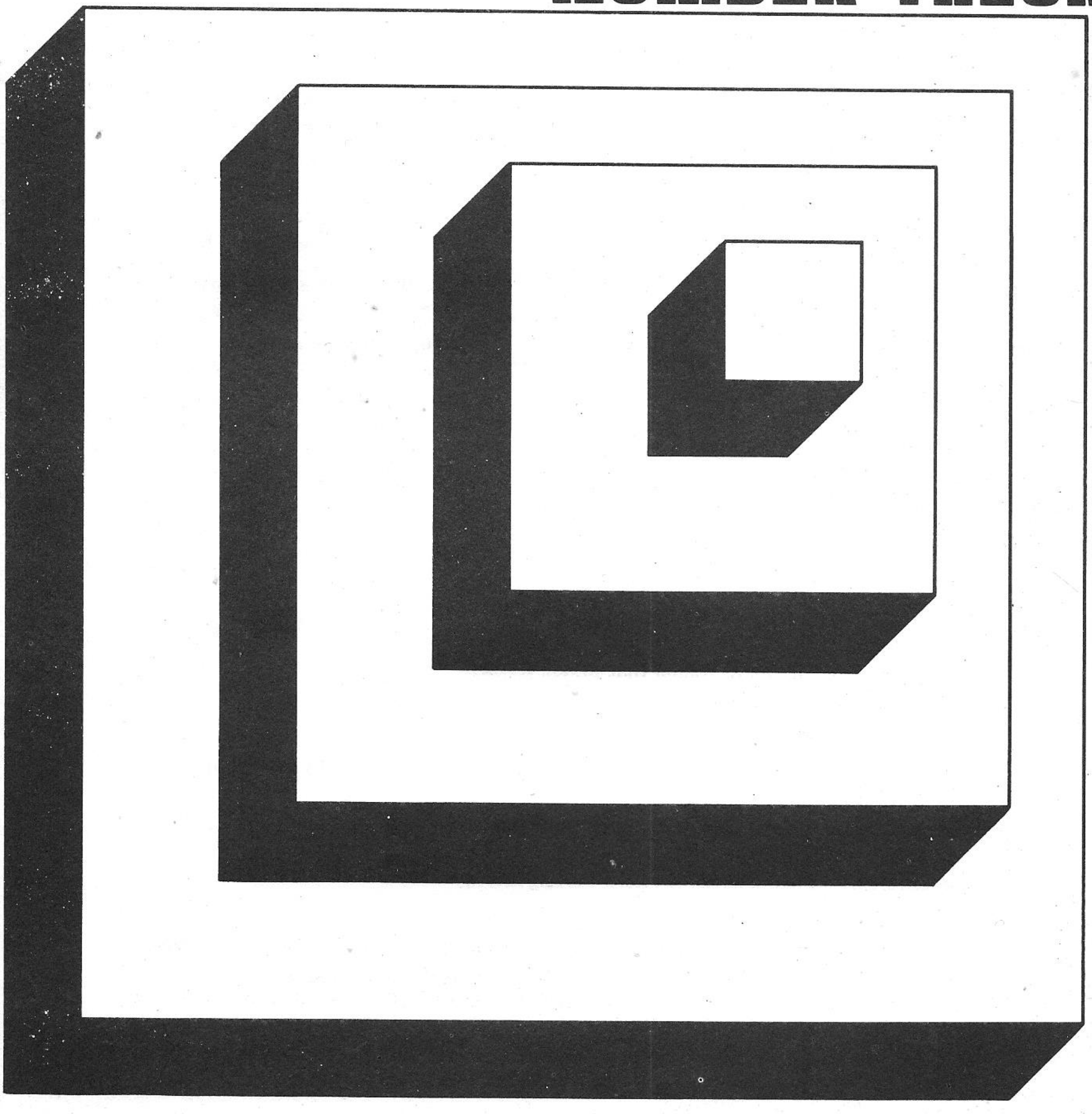
UNITS 5-8



THE OPEN UNIVERSITY
Mathematics: A Third Level Course
M335 Studies in Pure Mathematics
Prepared by the Course Team

NUMBER THEORY

UNITS 5-8



Proviso

Before starting work on this option read the M335 Course Guide. Also, be sure you have a copy of the 1980 (Open University) edition of the set book, *Elementary Number Theory*, by David M. Burton, published by Allyn & Bacon.

The Open University Press, Walton Hall, Milton Keynes.

First published 1981. Reprinted 1985.

Copyright © 1981 The Open University.

All rights reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the publishers.

Designed by the Graphic Design Group of the Open University.

Produced in Great Britain by
Speedlith Photo Litho Limited, Longford Trading Estate, Manchester M32 0JT.

ISBN 0 335 14011 4

This text forms part of the correspondence element of an Open University Third Level Course.

For general availability of supporting material referred to in this text, please write to Open University Educational Enterprises Limited, 12 Cofferidge Close, Stony Stratford, Milton Keynes MK11 1BY, Great Britain.

Further information on Open University courses may be obtained from The Admissions Office, The Open University, P.O. Box 48, Milton Keynes MK7 6AB.

Contents

Unit 5 Multiplicative Functions

5.0 Introduction **6**
5.1 The Functions τ and σ **6**
5.2 The Greatest Integer Function **11**
5.3 Euler's ϕ-function **13**
5.4 Euler's Theorem **17**
5.5 Summary **20**

Unit 6 The Quadratic Reciprocity Law

6.0 Introduction **22**
6.1 Euler's Criterion **22**
6.2 The Legendre Symbol **28**
6.3 Gauss' Lemma **30**
6.4 Quadratic Reciprocity (Tape Section) **33**
6.5 Summary **41**

Unit 7 Continued Fractions

7.0 Introduction **44**
7.1 Finite Continued Fractions **47**
7.2 Infinite Continued Fractions **53**
7.3 The Continued Fraction Algorithm **56**
7.4 The Continued Fractions of Quadratic Irrationals **61**
7.5 Rational Approximations **65**
7.6 Summary **68**

Unit 8 Diophantine Equations

8.0 Introduction **70**
8.1 Pell's Equation **71**
8.2 The Pythagorean Equation **73**
8.3 Fermat's Last Theorem **77**
8.4 Sums of Squares **79**
8.5 Summary **86**

UNIT 5
MULTIPLICATIVE FUNCTIONS

5.0 Introduction

Any function whose domain is the set of positive integers is called a *number-theoretic* or *arithmetic function*. Most of the number-theoretic functions which we shall meet also have the set of positive integers as codomain.

A number-theoretic function f which has the property that $f(mn) = f(m)\,f(n)$, whenever m and n are relatively prime integers, is said to be a *multiplicative function*. It is a simple inductive consequence of this definition that if f is multiplicative and n has prime factorization $n = p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ then $f(n) = f(p_1^{k_1})\,f(p_2^{k_2})\ldots f(p_r^{k_r})$. Thus, to determine a multiplicative function completely, we require to know its value at each prime power.

There are numerous interesting multiplicative functions which arise from looking at the divisors of an integer n. For instance, for any non-negative integer i, the function

$$f_i(n) = \sum d^i,$$

where the summation is taken over all the positive divisors d of n, can be shown to be multiplicative. The first two of these, f_0 and f_1, are very famous functions. f_0, which we rename τ, is the function which counts the number of positive divisors of each positive integer $n \geq 1$. f_1, which we rename σ, is the function which adds the positive divisors of each integer $n \geq 1$. These two functions τ and σ and their properties are discussed in Section 5.1.

Section 5.2 investigates properties of the greatest integer function. Although this function is not number-theoretic, because of its importance in number theory it holds a natural place in this unit.

Probably the best known of all multiplicative functions is Euler's ϕ-function, which assigns to each positive integer n the number of integers in a complete set of residues which are relatively prime to n. Section 5.3 introduces the ϕ-function and proves that it is multiplicative. Section 5.4 looks at properties of the ϕ-function and presents Euler's generalization of Fermat's Little Theorem, a result which is arguably one of the most useful in the whole of number theory.

The student with some background in algebra may well recognize that much of the material in Sections 5.3 and 5.4 could be set in the wider context of group theory. We have made several remarks to this effect in the unit. However, the emphasis of the course remains with 'numbers' and these algebraic asides can be ignored safely.

The unit comprises Sections 6.1, 6.3, 7.2 and 7.3 of **B**.

5.1 The Functions τ and σ

In this section we introduce the idea of multiplicative functions and meet our first two examples: the functions τ and σ.

Theorem 6-1 of **B**, in the first reading passage, ought to be familiar, as this result occurred in *Unit 2* when we were looking at the canonical prime factorization of positive integers.

READ B Section 6.1, page 110 as far as page 114, line -7.

NOTES (i) *Page 110, line -5*
By definition, an integer $n > 1$ is prime if and only if it has exactly two positive divisors, namely itself and 1. That is, n is prime if and only if $\tau(n) = 2$, or alternatively $\sigma(n) = n + 1$.

(ii) *Page 112, line −4*

When the product is expanded, the result is a sum of terms each of which is a product of r factors, one from each of the brackets. (In fact, there will be $(k_1+1)(k_2+1)\ldots(k_r+1)=\tau(n)$ terms.) In other words, the product is the sum of the $\tau(n)$ distinct terms of the form $p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, where $0 \le a_i \le k_i$, and by Theorem 6-1, this sum is precisely $\sigma(n)$.

(iii) *Page 114, line 14*

For an illustration, take $n = 18$. As d runs through the $\tau(18)$ divisors 1, 2, 3, 6, 9 and 18, so $d' = \dfrac{18}{d}$ takes the values 18, 9, 6, 3, 2 and 1 respectively. So

$$\prod_{d\mid 18} d = \prod_{d'\mid 18} d' = 1\cdot 2\cdot 3\cdot 6\cdot 9\cdot 18.$$

Multiplying the $\tau(18) = 6$ equations of the form $18 = dd'$ together gives

$$18^6 = \left(\prod_{d\mid 18} d\right)\left(\prod_{d'\mid 18} d'\right) = (1\cdot 2\cdot 3\cdot 6\cdot 9\cdot 18)^2$$

showing that the product of the positive divisors of 18 is equal to 18^3. ▲

As an example, let us look at the Problem quoted.

EXAMPLE 1 **B** page 118, Problems 6.1, number 7.

(a) We use Theorem 6-2 and SAQ 4 of *Unit 2*. If n is a perfect square, then the exponents in the prime factorization of n are even, i.e. $n = p_1^{2l_1}p_2^{2l_2}\cdots p_r^{2l_r}$. Therefore

$$\tau(n) = (2l_1+1)(2l_2+1)\cdots(2l_r+1)$$

is a product of odd integers, which is odd.

On the other hand, if n is not a perfect square, then at least one exponent in the prime factorization $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ is odd, so at least one factor in the product

$$(k_1+1)(k_2+1)\cdots(k_r+1) = \tau(n)$$

is even, and hence $\tau(n)$ is even.

(Alternatively, without appealing to Theorem 6-2, we could observe that if d is a divisor of n then so is $\dfrac{n}{d}$, since $n = d\cdot\left(\dfrac{n}{d}\right)$. This means that the divisors of n fall naturally into pairs, and hence $\tau(n)$ is even, unless there is a divisor d of n such that $d = \dfrac{n}{d}$. This in turn means $n = d^2$, i.e. n is a perfect square.)

(b) Let n have prime factorization $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. The formula at the foot of page 112 of **B** gives

$$\sigma(n) = \prod_{1\le i\le r}(1 + p_i + p_i^2 + \cdots + p_i^{k_i}).$$

For $\sigma(n)$ to be odd, each factor in this product must be odd. Following the given hint, if p_i is odd then $1 + p_i + p_i^2 + \cdots + p_i^{k_i}$ is odd precisely when k_i is even, whilst if $p_i = 2$ then this term is odd for any value of k_i. Therefore $\sigma(n)$ is odd if and only if the exponent of every odd prime in the factorization of n is even, that is, $n = 2^k p_2^{2l} p_3^{2l_3}\cdots p_r^{2l_r}$. But then, if k is even,

$$n = (2^{k/2}p_2^{l_2}p_3^{l_3}\cdots p_r^{l_r})^2, \qquad \text{a perfect square;}$$

whilst if k is odd,

$$n = 2(2^{\frac{k-1}{2}}p_2^{l_2}p_3^{l_3}\cdots p_r^{l_r})^2, \qquad \text{twice a perfect square.}$$

Hence $\sigma(n)$ is odd precisely when n is a perfect square or twice a perfect square.

SAQ 1 **B** page 118, Problems 6.1, number 8.

SAQ 2 **B** page 119, Problems 6.1, number 9.
(n is 'square-free' if it is not divisible by the square of any integer greater than 1.)

SAQ 3 **B** page 119, Problems 6.1, number 12.

SAQ 4 If $\tau(n) = p^3$, where p is prime, describe the possible prime factorizations of n. Hence find the smallest positive integer n for which (i) $\tau(n) = 8$ and (ii) $\tau(n) = 27$.

SOLUTION TO SAQ 1 Let the positive divisors of n be $d_1, d_2, \ldots, d_r$. Then

$$\sum_{d|n} \frac{1}{d} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_r}$$

$$= \frac{\dfrac{n}{d_1} + \dfrac{n}{d_2} + \cdots + \dfrac{n}{d_r}}{n}$$

$$= \frac{\sigma(n)}{n}.$$

(As d runs through the divisors of n, so does $\dfrac{n}{d}$ and so the numerator is $\sigma(n)$.) ■

SOLUTION TO SAQ 2 If n is square-free it is not divisible by the square of any prime, so the exponents in the prime factorization of n are all 1, i.e. $n = p_1 p_2 \cdots p_r$ for distinct primes $p_1, p_2, \ldots, p_r$. Theorem 6-2 (a) now gives $\tau(n) = 2^r$ as required. ■

SOLUTION TO SAQ 3 (a) If n has prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then Theorem 6-2 (a) shows that $\tau(n)$ is the product of r factors of the type $(k_i + 1)$, each of which must be at least 2. As 10 cannot be expressed as the product of more than two such factors, we know that $\tau(n) = 10$ implies that $r = 1$ or $r = 2$.

When $r = 1$, $\tau(n) = k_1 + 1 = 10$ gives $k_1 = 9$. So any integer n of the form $n = p^9$ has $\tau(n) = 10$.

When $r = 2$, $\tau(n) = (k_1 + 1)(k_2 + 1) = 10 = 2 \cdot 5$ gives $k_1 = 1$ and $k_2 = 4$ (or vice-versa). So any integer n of the form $n = p_1 p_2^4$ has $\tau(n) = 10$. The smallest value occurs when $n = 3 \cdot 2^4 = 48$.

(b) Using the hint, we know that if $\sigma(n) = 10$ then $1 \leq n \leq 9$, so it remains to check only that $\sigma(n) \neq 10$ for these nine values of n. The successive values of $\sigma(n)$ are 1, 3, 4, 7, 6, 12, 8, 15 and 13. ■

SOLUTION TO SAQ 4 There are three ways in which p^3 can be expressed as a product of factors each greater than 1, namely $p \cdot p \cdot p$, $p \cdot p^2$ and p^3. Accordingly, $\tau(n) = p^3$ arises when n is one of the forms $p_1^{p-1} p_2^{p-1} p_3^{p-1}$, $p_1^{p-1} p_2^{p^2-1}$ and $p_1^{p^3-1}$ (this by Theorem 6-2 (a)), where p_1, p_2, p_3 are distinct primes.

(i) $\tau(n) = 8 = 2^3$ arises when $n = p_1 p_2 p_3$, or $n = p_1 p_2^3$ or $n = p_1^7$. The least integer n of one of these forms is $3 \cdot 2^3 = 24$.

(ii) $\tau(n) = 27 = 3^3$ arises when $n = p_1^2 p_2^2 p_3^2$, or $n = p_1^2 p_2^8$ or $n = p_1^{26}$. The least integer n of one of these forms is $2^2 \cdot 3^2 \cdot 5^2 = 900$. ■

READ B page 114, line −6 to the end of Section 6.1.

NOTES (i) *Page 115, line 12*
The use of f in **B** might be slightly confusing here. On the previous line, he refers to the specific function given by $f(n) = 1$ for all $n \geq 1$, observing it to

be a simple example of a multiplicative function. Now we revert to an *arbitrary* multiplicative function f, showing how Definition 6-2 can be extended to the product of any number of positive integers which are pairwise relatively prime (that is, for which any two are relatively prime).

(ii) *Page 116, line 15*
In the statement of the Lemma, **B** includes the hypothesis 'and gcd $(d_1, d_2) = 1$'. Whilst it is important to appreciate that the divisors d_1 and d_2 are relatively prime, the inclusion of this statement is unnecessary since it follows automatically from the hypotheses gcd $(m, n) = 1$, $d_1 | n$ and $d_2 | m$. ▲

EXAMPLE 2 **B** page 120, Problems 6.1, number 22.

(a) Putting $s = 0$, and 1, respectively, we have

$$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1 = \tau(n),$$

and

$$\sigma_1(n) = \sum_{d|n} d^1 = \sum_{d|n} d = \sigma(n).$$

(b) The function f defined by $f(n) = n^s$ is multiplicative since $f(mn) = (mn)^s = m^s n^s = f(m)\,f(n)$ for *all* integers m and n, which certainly includes the case of m and n being relatively prime. (Functions like this which possess the multiplicative property for all pairs of positive integers are called *completely multiplicative functions.*)

We can now apply Theorem 6-4 to see that

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} d^s = \sigma_s(n)$$

is multiplicative.

(c) Let p^k be any prime power. The positive divisors of p^k are $1, p, p^2, \ldots, p^k$ and so

$$\begin{aligned}\sigma_s(p^k) &= 1^s + p^s + p^{2s} + \cdots + p^{ks}\\ &= \frac{(p^s)^{k+1} - 1}{p^s - 1} \qquad \text{(by SAQ 2 of } \textit{Unit 1}\text{, with } a = 1,\ r = p^s).\end{aligned}$$

Using the multiplicative property,

$$\begin{aligned}\sigma_s(n) &= \sigma_s(p_1^{k_1})\sigma_s(p_2^{k_2})\cdots\sigma_s(p_r^{k_r})\\ &= \left(\frac{p_1^{s(k_1+1)} - 1}{p_1^s - 1}\right)\left(\frac{p_2^{s(k_2+1)} - 1}{p_2^s - 1}\right)\cdots\left(\frac{p_r^{s(k_r+1)} - 1}{p_r^s - 1}\right).\end{aligned}$$

As a numerical illustration of this formula, let us determine the sum of the cubes of the divisors of 40.

$$\begin{aligned}\sigma_3(40) = \sigma_3(2^3 \cdot 5) &= \left(\frac{2^{12} - 1}{2^3 - 1}\right)\left(\frac{5^6 - 1}{5^3 - 1}\right)\\ &= (2^6 + 1)\cdot(2^3 + 1)\cdot(5^3 + 1)\\ &\quad \text{(using } a^{2m} - 1 = (a^m - 1)(a^m + 1) \text{ three times)}\\ &= 73710.\end{aligned}$$

SAQ 5 **B** page 119, Problems 6.1, number 14.

SAQ 6 **B** page 120, Problems 6.1, number 20.

SOLUTION TO SAQ 5

(a) From Theorem 6-2 (b), if $n = 2^{k-1}$

$$\sigma(n) = \frac{2^{(k-1)+1} - 1}{2-1} = 2^k - 1 = 2n - 1.$$

(b) If $2^k - 1$ is prime then $\sigma(2^k - 1) = (2^k - 1) + 1 = 2^k$, and from part (a), $\sigma(2^{k-1}) = 2^k - 1$. Now since gcd $(2^{k-1}, 2^k - 1) = 1$,

$$\sigma(n) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)2^k = 2n.$$

(An alternative method of proof would be to use Theorem 6-2 (b).)

(c)
$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1})\sigma(2^k - 3) \qquad &&(\text{since gcd } (2^{k-1}, 2^k - 3) = 1)\\ &= (2^k - 1)(2^k - 3 + 1) &&(\text{since } 2^k - 3 \text{ is prime})\\ &= 2^k(2^k - 3) + 2 = 2n + 2. && \blacksquare \end{aligned}$$

SOLUTION TO SAQ 6

(a) First note that the definition of ρ may be rephrased as $\rho(n) = 2^r$ where r is the number of distinct primes that divide n. Now if gcd $(m, n) = 1$, then there is no prime which divides both m and n, so if r distinct primes divide n, and s distinct primes divide m, there are $r + s$ distinct primes dividing mn. Therefore

$$\rho(mn) = 2^{r+s} = 2^s 2^r = \rho(m)\rho(n),$$

showing ρ to be multiplicative.

(b) $F(n) = \sum_{d|n} \rho(d)$ is multiplicative, by part (a) and Theorem 6-4. Now let n have prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, so that

$$\begin{aligned} F(n) &= F(p_1^{k_1})F(p_2^{k_2})\cdots F(p_r^{k_r})\\ &= \left(\sum_{d|p_1^{k_1}} \rho(d)\right)\left(\sum_{d|p_2^{k_2}} \rho(d)\right)\cdots\left(\sum_{d|p_r^{k_r}} \rho(d)\right). \end{aligned}$$

Our remaining task is to calculate $\sum_{d|p^k} \rho(d)$ for a general prime power p^k. Now the only divisors of p^k are $1, p, p^2, \ldots, p^k$ so

$$\begin{aligned} \sum_{d|p^k} \rho(d) &= \rho(1) + \rho(p) + \rho(p^2) + \cdots + \rho(p^k)\\ &= 1 + 2 + 2 + \cdots + 2\\ &\qquad (\text{since } p \text{ is the only prime dividing } p^r,\ r \geq 1)\\ &= 2k + 1. \end{aligned}$$

Therefore

$$F(n) = (2k_1 + 1)(2k_2 + 1)\cdots(2k_r + 1). \quad \blacksquare$$

In SAQ 5 (b) we found that all integers n of the form $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime, have the property that $\sigma(n) = 2n$. That is $n(=\sigma(n) - n)$ is equal to the sum of all its positive divisors except itself; for example $\sigma(6) = 12$ or, alternatively, $6 = 1 + 2 + 3$. Integers n with this property, $\sigma(n) = 2n$, are called *perfect numbers*. The four smallest perfect numbers are 6, 28, 496 and 8128, which are all integers of the above form, $2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime, corresponding respectively to $k = 2, 3, 5$ and 7.

Perfect numbers first aroused the interest of the Pythagoreans, and the result of SAQ 5(b) appears as Proposition 36 of Book IX of Euclid's *Elements*. The history of the search for perfect numbers, and the many conjectures about them, makes fascinating reading. There are no known *odd* perfect numbers and though considerable inroads have now been made into proving that there are none, a complete proof is still awaited. On the other hand, it was shown by Euler that the perfect numbers of the form $2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime, are the *only* even perfect numbers (see SAQ 7).

This result is not the end of the matter, for we are left with the problem of deciding which values of k make $2^k - 1$ prime. The numbers $M_k = 2^k - 1$ are called *Mersenne numbers* and if M_k is prime it is called a *Mersenne prime*. If k is composite, the Mersenne number M_k is easily shown to be composite, using the fact that $2^r - 1$ divides $2^{rs} - 1$, so the only candidates for Mersenne primes are the numbers M_p, where p is prime. As commented above, for the first four primes, M_p turns out to be prime also. However, the hypothesis that M_p might always be prime is refuted by the fact that M_{11} is composite. Because of continued interest, over the years, in the problem of finding Mersenne primes, the largest known prime has always been a Mersenne prime. As of mid-1979, the largest known prime is M_{44497}, which has 13395 digits. (Although it is known that there are infinitely many primes it is often difficult to decide whether a given large integer is prime or not!)

Chapter 10 of **B** is concerned with the search for perfect numbers and Mersenne primes and, although we have omitted it from this course, if you have time we would recommend you to read it. The chapter is much concerned with the historical development and, omitting some of the technical details of proofs, it is very readable. In any case, to appreciate the difficulty of finding Mersenne primes, you might find the anecdote in the second paragraph on page 226 stimulating. (Incidentally, Chapter 10 rounds off by mentioning another historically interesting family of integers: the *Fermat numbers* $F_n = 2^{2^n} + 1$. As F_1, F_2, F_3 and F_4 are all primes (and F_5 is very large), the conjecture was voiced for some time that all Fermat numbers are prime. But to this day no other Fermat primes have been found and there is a suspicion that all subsequent Fermat numbers are composite—a glance at page 236, line -9, will illustrate the difficulty of finding factorizations of 'small' Fermat numbers.)

SAQ 7 (In this exercise, we shall prove that every even perfect number n is of the form $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime.)

Let n be an even perfect number, and write $n = 2^{k-1}m$, where $k \geq 2$ and m is odd. Show that the requirement that n is perfect ($\sigma(n) = 2n$) gives

$$2^k m = (2^k - 1)\sigma(m).$$

Deduce from this that $(2^k - 1)|m$, and, putting $M = \dfrac{m}{2^k - 1}$, establish that $M = 1$ and $2^k - 1 = m$ is prime.

SOLUTION TO SAQ 7 See Theorem 10-1 on page 220 of **B**. The proof begins with the converse result, which is our SAQ 5(b). ■

5.2 The Greatest Integer Function

Though not a number-theoretic function, the greatest integer function will prove extremely useful to us in *Unit 6*. For this reason, we follow **B** in studying this function next. We shall, however, omit those results for which we do not have immediate use.

There is a slight conflict in that the notation used by **B** for the greatest integer function is the same as our earlier usage for congruence classes. The square bracket notation is quite standard for both these contexts. No confusion should arise, since congruence classes appear only when we are dealing exclusively with integers, whilst the domain of the greatest integer function is the set of all real numbers.

READ B Section 6.3, page 126 as far as the foot of page 128.

NOTES (i) *Page 126, line 13*
In fact, $[x]$ is the unique integer n which satisfies $x = n + \theta$ with $0 \leq \theta < 1$, since this implies that $x - 1 < n \leq x$.

(ii) *Page 126, line* -4
To illustrate the proof of Theorem 6-9, look at the particular case when $n = 37$ and $p = 3$. Our objective is to find the exponent of the highest power of 3 which divides $37! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 36 \cdot 37$. Since 3 is prime, we can obtain this power by adding together the powers of 3 which divide the factors $1, 2, 3, \ldots, 37$. Of these factors, twelve are divisible by 3:

$$3(=1 \cdot 3), \quad 6(=2 \cdot 3), \quad \ldots, \quad 33(=11 \cdot 3), \quad 36(=12 \cdot 3).$$

That there are twelve factors divisible by 3 comes from the fact that $36 = 12 \cdot 3$ is the largest multiple of 3 which is less than or equal to 37; in other words, because $12 = [\frac{37}{3}]$.

So we know $3^{12} | 37!$ However, four of the factors of 37! are divisible by 3^2:

$$9(=1 \cdot 3^2), \quad 18(=2 \cdot 3^2), \quad 27(=3 \cdot 3^2), \quad 36(=4 \cdot 3^2).$$

That there are four such factors comes from the fact that $36 = 4 \cdot 3^2$ is the largest multiple of 3^2 which is less than or equal to 37; that is, $4 = [\frac{37}{3^2}]$.

Each of the above four factors contributes one more to the exponent of 3 in 37! so that we now know $3^{12+4} | 37!$ Finally, $27 = 1 \cdot 3^3$ is actually divisible by 3^3 and so contributes a further $1 = [\frac{37}{3^3}]$ to the exponent of 3 in 37! So the total exponent is $12 + 4 + 1 = [\frac{37}{3}] + [\frac{37}{3^2}] + [\frac{37}{3^3}]$.

(iii) *Page 128, line 7*
That $[a + b] \geq [a] + [b]$ is one of the results we ask you to prove in SAQ 8, which is intended to familiarize you with the greatest integer function.

(iv) *Page 128, line 11*
To illustrate formula (1), let us look at the example $n = 37$, $p = 3$, $r = 11$. The inequalities for the successive values of k are

$$\begin{array}{lll} k = 1 & [\frac{37}{3}] \geq [\frac{11}{3}] + [\frac{26}{3}]; & 12 \geq 3 + 8 \\ k = 2 & [\frac{37}{9}] \geq [\frac{11}{9}] + [\frac{26}{9}]; & 4 \geq 1 + 2 \\ k = 3 & [\frac{37}{27}] \geq [\frac{11}{27}] + [\frac{26}{27}]; & 1 \geq 0 + 0 \end{array}$$

and for subsequent values of k every term is 0. Adding:

$$\sum_{k=1}^{\infty} [\tfrac{37}{3^k}] \geq \sum_{k=1}^{\infty} [\tfrac{11}{3^k}] + \sum_{k=1}^{\infty} [\tfrac{26}{3^k}]; \qquad 17 \geq 4 + 10.$$

Now, by Theorem 6-9, $\sum_{k=1}^{\infty} [\frac{37}{3^k}]$ is the exponent of the highest power of 3 which divides 37! Similarly, the terms on the right-hand side of the inequality are the exponents of the highest power of 3 dividing 11! and 26! respectively. The right-hand side therefore gives the exponent of the highest power of 3 dividing the product (11!) (26!), namely 3^{4+10}, and the inequality tells us that this is not greater than the highest power of 3 dividing 37!, namely 3^{17}. ▲

SAQ 8 **B** pages 130 and 131, Problems 6.3, number 2 parts (a), (b), (c), (d) and (e).

SAQ 9 **B** page 131, Problems 6.3, number 5.

SOLUTION TO SAQ 8

(a) Let $x = [x] + \theta$, where $0 \leq \theta < 1$. It follows that $x + n = ([x] + n) + \theta$, where $[x] + n$ is an integer and $0 \leq \theta < 1$, and so $[x + n] = [x] + n$.

(b) If x is an integer, then so is $-x$, which means that $[x] = x$ and $[-x] = -x$. Therefore $[x] + [-x] = x - x = 0$. If x is not an integer then $x = [x] + \theta$, where $0 < \theta < 1$, and so, using the hint, $-x = -[x] - 1 + (1 - \theta)$. Now $-[x] - 1$ is an integer and $0 < 1 - \theta < 1$, therefore $[-x] = -[x] - 1$, giving $[x] + [-x] = -1$.

(c) $[x] \le x$ and $[y] \le y$ imply that $[x] + [y] \le x + y$. Now $[x + y]$ is the greatest integer less than or equal to $x + y$, and, as $[x] + [y]$ is an integer and $[x] + [y] \le x + y$, we have $[x] + [y] \le [x + y]$.

Writing $x = [x] + \theta$ and $y = [y] + \phi$, where $0 \le \theta, \phi < 1$, $xy = [x][y] + \theta[y] + \phi[x] + \theta\phi$. Since x and y are positive, $[x] \ge 0$ and $[y] \ge 0$, and consequently $\theta[y] + \phi[x] + \theta\phi \ge 0$. Therefore $xy \ge [x][y]$, but since $[xy]$ is the greatest integer which is less than or equal to xy, $[xy] \ge [x][y]$.

(d) Using the hint, we write $\dfrac{x}{n} = \left[\dfrac{x}{n}\right] + \theta$ where $0 \le \theta < 1$, so that $x = n\left[\dfrac{x}{n}\right] + n\theta$ and hence by part (a) (since $n\left[\dfrac{x}{n}\right]$ is an integer), $[x] = n\left[\dfrac{x}{n}\right] + [n\theta]$. Now $0 \le n\theta < n$, so $0 \le [n\theta] < n$ and $0 \le \dfrac{[n\theta]}{n} < 1$.

Hence $\dfrac{[x]}{n} = \left[\dfrac{x}{n}\right] + \dfrac{[n\theta]}{n}$, where $\left[\dfrac{x}{n}\right]$ is an integer and $0 \le \dfrac{[n\theta]}{n} < 1$; therefore $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$.

(e) $\left[\dfrac{m}{k}\right] \le \dfrac{m}{k}$, therefore $n\left[\dfrac{m}{k}\right] \le \dfrac{nm}{k}$, so $n\left[\dfrac{m}{k}\right]$ is an integer less than or equal to $\dfrac{nm}{k}$ and hence $n\left[\dfrac{m}{k}\right] \le \left[\dfrac{nm}{k}\right]$. ■

SOLUTION TO SAQ 9 Following Example 6-2, we could use Theorem 6-9 to find the highest power of each of the primes 2 and 5 dividing 1000! and the required answer will be the smaller of these two exponents. However, it is abundantly clear from the formula that 5 has the smaller exponent and so the number of zeroes in which 1000! terminates is

$$\left[\tfrac{1000}{5}\right] + \left[\tfrac{1000}{25}\right] + \left[\tfrac{1000}{125}\right] + \left[\tfrac{1000}{625}\right] = 200 + 40 + 8 + 1 = 249.$$

(If you care to check, you will find that the exponent of 2 is 994.) ■

5.3 Euler's ϕ-function

The Euler ϕ-function is probably the most important of all multiplicative functions. For each positive integer n, it counts the number of integers from 1 to n inclusive which are relatively prime to n. So, for example, $\phi(4) = 2$ since 1 and 3 are relatively prime to 4, and $\phi(5) = 4$ since 1, 2, 3 and 4 are relatively prime to 5.

COMMENT From the point of view of group theory, the ϕ-function arises as follows. We have already seen that $\mathbb{Z}_n$ is a group with binary operation $+$, so it seems natural to investigate $\mathbb{Z}_n$ with binary operation $\times$. We quickly see that a group does not result because, although $\times$ is closed and associative on $\mathbb{Z}_n$ and $[1][x] = [x]$ shows that $[1]$ is a multiplicative identity, not all elements have multiplicative inverses. For instance, since $[0][x] = [0]$ for all x, $[0]$ does not have an inverse (except in $\mathbb{Z}_1$ where $[0] = [1]$). In fact, the situation is worse. For example, in $\mathbb{Z}_4$, $[2]$ does not have an inverse since $[2][0] = [0]$, $[2][1] = [2]$, $[2][2] = [0]$ and $[2][3] = [2]$.

But what about the subset U_n of $\mathbb{Z}_n$ consisting of those elements which do have multiplicative inverses, the so-called *units* of $\mathbb{Z}_n$? In this case, it is not difficult to show that the product of two units is a unit (closure), and then the associativity, identity and inverse axioms follow immediately. So U_n is a group under binary operation $\times$.

Which elements are the units of $\mathbb{Z}_n$? $[x]$ is a unit of $\mathbb{Z}_n$ if and only if there is an integer a such that $[x]\,[a] = [1]$, or what amounts to the same thing, $xa \equiv 1 \pmod{n}$. This, in turn, can be re-expressed as $xa + nb = 1$, for some integer b. Now Theorem 2-4 on page 27 of **B** shows that this is the case if and only if x is relatively prime to n. So there are $\phi(n)$ units in $\mathbb{Z}_n$, corresponding to the least positive residues of n which are relatively prime to n, and $\phi(n)$ is the order of the multiplicative group of units, U_n.

READ B Sections 7.1 and 7.2, pages 134–140.

NOTES (i) *Page 138, line −6*

The proof of Theorem 7-2 may be clearer if we look at a particular case. If we take $m = 9$ and $n = 8$ the array is:

①	2	~~3~~	4	⑤	~~6~~	⑦	8	~~9~~
10	⑪	~~12~~	⑬	14	~~15~~	16	⑰	~~18~~
⑲	20	~~21~~	22	㉓	~~24~~	㉕	26	~~27~~
28	㉙	~~30~~	㉛	32	~~33~~	34	㉟	~~36~~
㊲	38	~~39~~	40	㊶	~~42~~	㊸	44	~~45~~
46	㊼	~~48~~	㊾	50	~~51~~	52	(53)	~~54~~
(55)	56	~~57~~	58	(59)	~~60~~	(61)	62	~~63~~
64	(65)	~~66~~	(67)	68	~~69~~	70	(71)	~~72~~

In each column the entries are of the form $r, 9 + r, 2 \cdot 9 + r, \ldots, 7 \cdot 9 + r$, and are therefore congruent to each other modulo $m = 9$. So as far as being relatively prime to 9 is concerned, all the elements in a column behave the same way. We can therefore discard all the elements in the columns headed 3, 6, and 9, since those are not relatively prime to 9, and concentrate on the $\phi(m) = \phi(9) = 6$ columns headed by the integers relatively prime to 9, i.e. 1, 2, 4, 5, 7 and 8.

From these remaining $\phi(m)$ columns, we now want to find which elements are relatively prime to $n = 8$. The key is in observing that, in each column, the n elements are congruent modulo n, to, in some order, 0, 1, $2, \ldots, 7 = n - 1$, since no two elements in a column can be congruent to one another modulo n. For example, in the column headed 4 we have $4 \equiv 4$, $13 \equiv 5$, $22 \equiv 6$, $31 \equiv 7$, $40 \equiv 0$, $49 \equiv 1$, $58 \equiv 2$ and $67 \equiv 3$ (modulo 8). It follows that in each of these $\phi(m)$ columns, there must be $\phi(n) = \phi(8) = 4$ elements relatively prime to n, and these are the circled elements in the array.

It follows that there are $\phi(m)\phi(n) = 6 \times 4 = 24$ elements relatively prime to $mn = 72$.

(ii) *Page 139, line 16*

Although **B** includes an inductive proof of Theorem 7-3, the result is immediate. From Theorem 7-2 we have

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \phi(p_1^{k_1})\,\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$$

and Theorem 7-1 now completes the argument. ▲

A word of warning. It is all too easy to remember

(i) $\phi(p) = p - 1$, p prime

and (ii) ϕ is multiplicative,

and yet make erroneous deductions such as

$$\phi(p^2) = \phi(p) \cdot \phi(p) = (p-1)^2.$$

Make sure you remember the 'pairwise relatively prime' condition in the definition of multiplicative functions.

To illustrate Euler's ϕ-function, we look at three examples.

EXAMPLE 3 **B** page 140, Problems 7.2, number 4.

(a) As n is odd, n and 2 are relatively prime. So

$$\phi(2n) = \phi(2)\,\phi(n) = \phi(n),$$

since $\phi(2) = 1$.

(b) Let $n = 2^r m$ where $r \geq 1$ and m is odd.

$$\phi(2n) = \phi(2^{r+1}m) = \phi(2^{r+1})\,\phi(m) = 2^r\phi(m),$$

and

$$2\phi(n) = 2\phi(2^r m) = 2\phi(2^r)\,\phi(m) = 2 \cdot 2^{r-1}\phi(m) = 2^r\phi(m).$$

Therefore $\phi(2n) = 2\phi(n)$.

(c) If $3|n$, put $n = 3^r m$ where $r \geq 1$ and $\gcd(3, m) = 1$. Then

$$\phi(3n) = \phi(3^{r+1}m) = \phi(3^{r+1})\,\phi(m) = 3^{r+1} \cdot \tfrac{2}{3} \cdot \phi(m) = 2 \cdot 3^r\phi(m),$$

and

$$3\phi(n) = 3\phi(3^r m) = 3 \cdot 3^r \cdot \tfrac{2}{3}\phi(m) = 2 \cdot 3^r\phi(m) = \phi(3n).$$

We are also asked to show, conversely, that if $\phi(3n) = 3\phi(n)$, then $3|n$. This is the same as showing that if $3 \nmid n$ then $\phi(3n) \neq 3\phi(n)$. This is an immediate consequence of our solution to part (d).

(d) If $3 \nmid n$, then $\gcd(3, n) = 1$ so

$$\phi(3n) = \phi(3)\,\phi(n) = 2\phi(n)\,(\neq 3\phi(n)).$$

Conversely, if $\phi(3n) = 2\phi(n)$, then $\phi(3n) \neq 3\phi(n)$ and so by part (c), $3 \nmid n$.

(e) If $n = 2^k$, $k \geq 1$, then $\phi(n) = \phi(2^k) = 2^{k-1} = \dfrac{n}{2}$. Conversely, suppose $\phi(n) = \dfrac{n}{2}$. Then since $\phi(n)$ is an integer, we know that $2|n$ and we can write $n = 2^k N$ where $k \geq 1$ and N is odd. Then $\phi(n) = \phi(2^k)\,\phi(N) = 2^{k-1}\phi(N)$. But $\phi(n) = \dfrac{n}{2} = 2^{k-1}N$ which gives $\phi(N) = N$. Now if $N > 1$ then

$\phi(N) = N\left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right) \cdots \left(1 - \dfrac{1}{p_r}\right) < N$, and so we conclude that

$N = 1$ and $n = 2^k$, as required.

EXAMPLE 4 **B** page 141, Problems 7.2, number 13.

Let n have prime factorization $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$. By Theorem 6-1, any divisor d of n has the form

$$d = p_1^{a_1}p_2^{a_2} \ldots p_r^{a_r}, \quad \text{where } 0 \leq a_i \leq k_i \text{ (for } i = 1, 2, \ldots, r).$$

From the multiplicative nature of ϕ,

$$\phi(n) = \phi(p_1^{k_1})\,\phi(p_2^{k_2})\ldots\phi(p_r^{k_r})$$

and

$$\phi(d) = \phi(p_1^{a_1})\,\phi(p_2^{a_2})\ldots\phi(p_r^{a_r}).$$

To deduce that $\phi(d)|\phi(n)$, it suffices to show that $\phi(p_i^{a_i})|\phi(p_i^{k_i})$, where $0 \le a_i \le k_i$. The case $a_i = 0$ is easily dealt with, since then $p_i^{a_i} = 1$ and $\phi(p_i^{a_i}) = 1$. On the other hand, if $a_i > 0$ then

$$\phi(p_i^{k_i}) = p_i^{k_i-1}\,(p^i - 1) = p_i^{k_i-a_i}\,p_i^{a_i-1}\,(p_i - 1) = p_i^{k_i-a_i}\,\phi(p_i^{a_i}).$$

EXAMPLE 5 **B** page 141, Problems 7.2, number 10.

If $p_1, p_2, \ldots, p_r$ are the distinct primes which divide m, then, since every prime dividing n also divides m, the same r primes are the ones which divide mn. Therefore

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right),$$

and

$$\phi(mn) = mn\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)$$

so $\phi(mn) = n\phi(m)$.

Putting $m = n$ we obtain $\phi(n^2) = n\phi(n)$.

SAQ 10 **B** page 140, Problems 7.2, number 1.

SAQ 11 **B** page 141, Problems 7.2, number 5.

SAQ 12 **B** page 142, Problems 7.2, number 17.
[Note that the square brackets in line 2 of the question do not refer to the greatest integer function.]

SAQ 13 **B** page 142, Problems 7.2, number 19.

SOLUTION TO SAQ 10 $1001 = 7 \cdot 11 \cdot 13$, so

$$\phi(1001) = 1001(1 - \tfrac{1}{7})(1 - \tfrac{1}{11})(1 - \tfrac{1}{13}) = 720.$$

$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, so

$$\phi(5040) = 5040(1 - \tfrac{1}{2})(1 - \tfrac{1}{3})(1 - \tfrac{1}{5})(1 - \tfrac{1}{7}) = 1152.$$

$36000 = 2^5 \cdot 3^2 \cdot 5^3$, so

$$\phi(36000) = 36000(1 - \tfrac{1}{2})(1 - \tfrac{1}{3})(1 - \tfrac{1}{5}) = 9600. \quad \blacksquare$$

SOLUTION TO SAQ 11

$$\phi(n) = \phi(2(2p - 1)) = \phi(2)\phi(2p - 1) = \phi(2p - 1) = 2p - 2,$$

since $2p - 1$ is prime.

$$\phi(n + 2) = \phi(4p) = \phi(4)\phi(p) = 2(p - 1) = 2p - 2,$$

since p is prime. So $\phi(n) = \phi(n + 2)$. $\blacksquare$

SOLUTION TO SAQ 12 Let $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ so that

$$\phi(n) = p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}(p_1 - 1)(p_2 - 1)\cdots(p_r - 1).$$

If $\phi(n) = 16$, then $(p_i - 1)|16$, so the only possible values for the p_i are 2, 3, 5 and 17. Furthermore, $p_i^{k_i-1}|16$ so either $p_i = 2$, or $k_i = 1$. Therefore n must be of the form $2^a3^b5^c17^d$ where b, c and d are either 0 or 1.

Suppose $d = 1$. Then $n = 17m$ and $\phi(n) = \phi(17)\phi(m) = 16\phi(m)$ so that $\phi(m) = 1$. Theorem 7-4 now implies that $m = 1$ or 2. It follows that 17 and 34 are the only solutions involving the prime 17.

We now assume $d = 0$, i.e. $n = 2^a 3^b 5^c$ where b and c are 0 or 1. Consider the case $c = 1$, so that $16 = \phi(n) = \phi(2^a 3^b)\,\phi(5) = 4\phi(2^a 3^b)$, giving $\phi(2^a 3^b) = 4$. For $b = 0$, this requires $a = 3$ and for $b = 1$, $a = 2$, giving respectively $n = 40$ and $n = 60$. Lastly, if $c = 0$, $n = 2^a 3^b$. For $b = 1$, $16 = \phi(n) = \phi(2^a)\,\phi(3) = 2^a$ giving $a = 4$ and $n = 48$. For $b = 0$, $16 = \phi(n) = \phi(2^a) = 2^{a-1}$ giving $a = 5$ and $n = 32$. So the only solutions of $\phi(n) = 16$ are $n = 17$, 32, 34, 40, 48 and 60.

Repeating the same arguments when $\phi(n) = 24$, we see that the primes involved this time are 2, 3, 5, 7 and 13, so that n is of the form $2^a 3^b 5^c 7^d 13^e$. Also, since $5 \nmid 24$, $7 \nmid 24$ and $13 \nmid 24$ we must have that c, d and e are equal to 0 or 1. Looking each time at the largest prime involved, the case $e = 1$ leads to solutions 39, 52 and 78, the case $d = 1$ leads to solutions 35, 56, 70 and 84, $c = 1$ gives 45 and 90, and finally $c = d = e = 0$ gives solution 72. ■

SOLUTION TO SAQ 13 $\phi(p^k) = p^{k-1}(p-1)$.
Therefore

$$\begin{aligned}\phi(\phi(p^k)) &= \phi(p^{k-1})\,\phi(p-1), \qquad \text{since } \gcd(p^{k-1}, p-1) = 1\\ &= p^{k-2}(p-1)\,\phi(p-1).\end{aligned}$$

Now in Example 5 we showed that $\phi(n^2) = n\phi(n)$, and so

$$(p-1)\,\phi(p-1) = \phi((p-1)^2)$$

giving

$$\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2). \quad ■$$

5.4 Euler's Theorem

The remaining two sections of Chapter 7 of **B** investigate properties of the ϕ-function. We shall study only Section 7.3, which is concerned with Euler's generalization of Fermat's Little Theorem.

COMMENT You may well recognize Euler's Theorem as being a particular case of a general result in group theory. Lagrange's Theorem (in group theory) tells us that if G is a finite group with order $|G|$ and g is any element of G, then the order of g divides $|G|$. An immediate corollary of this is that $g^{|G|} = e$, the identity element of G. Euler's Theorem is just this result for the case when G is the multiplicative group of units in $\mathbb{Z}_n$, whose order, as we remarked in the introduction to Section 5.3, is $\phi(n)$. To put the result in its right perspective, however, it must be remembered that Euler proved his result over a hundred years before the established birth of group theory.

READ B Section 7.3, page 142 as far as page 145, line 10.

SAQ 14 **B** page 147, Problems 7.3, number 1.

SAQ 15 Find the final two digits of 13^{122}.

SAQ 16 **B** page 147, Problems 7.3, number 3.

SAQ 17 **B** page 147, Problems 7.3, number 6.

SOLUTION TO SAQ 14 (a) It is sufficient to show that $a^{37} \equiv a \pmod{p}$ for each of the primes $p = 7$, 13 and 19, so in fact we need only use the Corollary to Fermat's Theorem, i.e. $a^p \equiv a \pmod{p}$.

$$a^{37} = (a^7)^5 a^2 \equiv a^5 a^2 \equiv a^7 \equiv a \pmod{7},$$

$$a^{37} = (a^{13})^2 a^{11} \equiv a^2 a^{11} \equiv a^{13} \equiv a \pmod{13}$$

and

$$a^{37} = a^{19} a^{18} \equiv a a^{18} \equiv a^{19} \equiv a \pmod{19}.$$

(b) Similar to (a). We use the Corollary to Fermat's Theorem to show that $a^{13} \equiv a \pmod{p}$ for $p = 2, 3, 5, 7$ and 13.

$$a^{13} = (a^2)^6 a \equiv a^6 a \equiv (a^2)^3 a \equiv a^3 a \equiv (a^2)^2 \equiv a^2 \equiv a \pmod{2},$$

$$a^{13} = (a^3)^4 a \equiv a^4 a \equiv a^3 a^2 \equiv a a^2 \equiv a^3 \equiv a \pmod{3},$$

$$a^{13} = (a^5)^2 a^3 \equiv a^2 a^3 \equiv a^5 \equiv a \pmod{5},$$

$$a^{13} = a^7 a^6 \equiv a a^6 \equiv a^7 \equiv a \pmod{7},$$

and

$$a^{13} \equiv a \pmod{13}.$$

(c) In this case we do need Euler's Theorem, to deal with the factor 16. Since $\phi(16) = 8$, we know that $a^8 \equiv 1 \pmod{16}$ for any integer a such that $\gcd(a, 16) = 1$, i.e. for any odd integer. So for any odd integer a we have

$$a^{33} = (a^8)^4 a \equiv 1^4 a \equiv a \pmod{16}.$$

To deal with the remaining prime factors we revert to the Corollary to Fermat's Theorem:

$$a^{33} = (a^3)^{11} \equiv a^{11} \equiv (a^3)^3 a^2 \equiv a^3 a^2 \equiv a a^2 \equiv a^3 \equiv a \pmod{3},$$

$$a^{33} = (a^5)^6 a^3 \equiv a^6 a^3 \equiv a^5 a^4 \equiv a a^4 \equiv a^5 \equiv a \pmod{5}$$

and

$$a^{33} = a^{17} a^{16} \equiv a a^{16} \equiv a^{17} \equiv a \pmod{17}.$$

This shows that $a^{33} \equiv a \pmod{3 \cdot 5 \cdot 17}$ for all integers a, and $a^{33} \equiv a \pmod{3 \cdot 5 \cdot 16 \cdot 17}$ for any odd integer a. ■

SOLUTION TO SAQ 15 We need to find the remainder on dividing 13^{122} by 100. Since $\phi(100) = 40$ and $\gcd(13, 100) = 1$, Euler's Theorem shows that $13^{40} \equiv 1 \pmod{100}$, and so $13^{122} = (13^{40})^3 \cdot 13^2 \equiv 13^2 \equiv 69 \pmod{100}$. Hence the final two digits of 13^{122} are 69. ■

SOLUTION TO SAQ 16 Since $\gcd(m, n) = 1$, we have $n^{\phi(m)} \equiv 1 \pmod{m}$ and $m^{\phi(n)} \equiv 1 \pmod{n}$. That is, $m | (n^{\phi(m)} - 1)$ and $n | (m^{\phi(n)} - 1)$, giving $mn | (n^{\phi(m)} - 1)(m^{\phi(n)} - 1)$. In other words, $mn | m^{\phi(n)} n^{\phi(m)} - m^{\phi(n)} - n^{\phi(m)} + 1$, and since $mn | m^{\phi(n)} n^{\phi(m)}$ this means that $mn | (-m^{\phi(n)} - n^{\phi(m)} + 1)$. That is, $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$. ■

SOLUTION TO SAQ 17 (a) Substituting $x = ba^{\phi(n)-1}$ we have

$$ax = aba^{\phi(n)-1} = ba^{\phi(n)} \equiv b \pmod{n}.$$

Thus $x = ba^{\phi(n)-1}$ is the (unique modulo n) solution of $ax \equiv b \pmod{n}$.

(b) $\phi(26) = 12$, and so the solution of $3x \equiv 5 \pmod{26}$ is

$$x = 5 \cdot 3^{11} = 5 \cdot (3^3)^3 \cdot 3^2 \equiv 5 \cdot 1^3 \cdot 3^2 \equiv 19 \pmod{26}.$$

$\phi(40) = 16$, and so the solution of $13x \equiv 2 \pmod{40}$ is

$$x = 2 \cdot 13^{15} = 2 \cdot (13^2)^7 \cdot 13 \equiv 2 \cdot 9^7 \cdot 13 \equiv 2 \cdot (9^2)^3 \cdot 9 \cdot 13 \equiv 18 \cdot 13 \equiv 34 \pmod{40}.$$

$\phi(49) = 42$, and so the solution of $10x \equiv 21 \pmod{49}$ is

$$x = 21 \cdot 10^{41} = 210 \cdot (10^2)^{20} \equiv 210 \cdot 2^{20} \equiv 14 \cdot (2^{10})^2$$

$$\equiv 14 \cdot (-5)^2 \equiv 7 \pmod{49}. \quad ■$$

READ B page 145, line 11 to the end of Section 7.3.

NOTES (i) *Page 145, line 13*

The second proof of Euler's Theorem should be read for interest and as an exercise in manipulation. The previous, simpler, proof is preferred.

(ii) *Page 146, line −3*
The Chinese Remainder Theorem is primarily concerned with the existence and uniqueness of a solution. However, here (as in the earlier proof on **B** page 87) the proof includes the construction of an actual simultaneous solution. But the solution produced will usually be inconveniently large and has to be reduced modulo $n_1 n_2 \ldots n_r$. For instance, consider the problem of solving simultaneously

$$x \equiv 1 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 12 \pmod{14}.$$

In this case, $N_1 = 70$, $N_2 = 42$, $N_3 = 15$, $\phi(n_1) = 2$, $\phi(n_2) = 4$ and $\phi(n_3) = 6$. The solution given (by line −9, page 146) is

$$x = 70^2 + 3 \cdot 42^4 + 12 \cdot 15^6 = 146027488$$

which reduces modulo 210 to 208.

So the method given here should be looked upon as theoretical; for practical purposes we revert to the technique of *Unit 3*. For the above problem:

$x \equiv 12 \pmod{14} \Rightarrow x = 12, 26, 40, 54, 68$ (increasing by 14 until division by 5 leaves remainder 3)

$\downarrow$

$x \equiv 3 \pmod 5 \Rightarrow$ $x = 68, 138, 208$ (increasing by $5 \cdot 14 = 70$ until division by 3 leaves remainder 1)

$\downarrow$

$x \equiv 1 \pmod 3 \Rightarrow$ $x = 208.$

(iii) *Page 147, line 9*
B remarks correctly that $7 | 111111$. However, if you follow through the case $n = 7$, what is actually proved is that 7 divides

$$\frac{10^{\phi(63)} - 1}{9} = \frac{10^{36} - 1}{9} = 111 \ldots 1 \qquad (36 \text{ ones}).$$

The argument presents a general proof of the claimed result for any integer n relatively prime to 10. This result can be tightened when n is prime, as we see in SAQ 18. ▲

SAQ 18 **B** page 147, Problems 7.3, number 7.

SOLUTION TO SAQ 18 Firstly, the result is certainly true for the prime 3 since by the divisibility test 3 divides every third term of the given sequence, namely, the terms consisting of 3 ones, 6 ones, 9 ones etc.

Suppose p is a prime other than 2, 3 or 5. Then by Euler's Theorem, since $\gcd(10, p) = 1$,

$$10^{\phi(p)} = 10^{p-1} \equiv 1 \pmod p;$$

that is, p divides $10^{p-1} - 1 = 999 \ldots 9$, the number consisting of $p - 1$ nines. Now since $p \neq 3$, $\gcd(9, p) = 1$ and by Euclid's Lemma, p divides $a = 111 \ldots 1$, the number consisting of $p - 1$ ones.

Now the number consisting of $2(p - 1)$ ones is $a + 10^{p-1} a$, so it also is divisible by p. Similarly, we see that p divides every $(p - 1)$th term of the given sequence, namely the terms consisting of $(p - 1)$ ones, $2(p - 1)$ ones, $3(p - 1)$ ones, and so on. ■

5.5 Summary

In this unit we have studied some of the important functions of number theory, the central theme being the multiplicative functions.

Section 5.1 was concerned with two functions, τ and σ. For any positive integer n, $\tau(n)$ is the number of positive divisors of n, and $\sigma(n)$ is the sum of those divisors. Both functions were shown to be multiplicative and we obtained the following formulae in terms of the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$:

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1),$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Pursuing the σ-function, we looked briefly at perfect numbers, which are positive integers n for which $\sigma(n) = 2n$. We classified the even perfect numbers as being those integers of the form $2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime. The primes of the form $2^k - 1$ are the Mersenne primes.

In Section 5.2, we investigated properties of the greatest integer function and in particular used the greatest integer function to find the prime factorization of $n!$

Section 5.3 introduced Euler's ϕ-function, $\phi(n)$, which assigns to each positive integer n the number of elements in the set of least positive residues which are relatively prime to n, ϕ was shown to be multiplicative and we obtained the formula

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right),$$

where $p_1, p_2, \ldots, p_r$ are the distinct primes dividing n.

Section 5.4 presented Euler's generalization of Fermat's Little Theorem and looked at numerous applications. Euler's Theorem states that if n is a positive integer and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 6
THE QUADRATIC RECIPROCITY LAW

6.0 Introduction

In Section 4.4 of *Unit 4*, pursuing applications of Fermat's Little Theorem, we began a study of the solvability of polynomial congruences. We discovered similarities with the solutions of polynomial equations in that, provided we take congruences to a prime modulus, a polynomial congruence of degree n has at most n incongruent solutions. We now pick up this thread again, the central theme of this unit being the solvability of the general quadratic congruence.

From the outset, we shall appreciate that the essential problem we must solve concerns the congruence

$$x^2 \equiv a \pmod{p}.$$

In other words, we need to know which elements in the arithmetic modulo p are the perfect squares. In the early units of the course, we solved such problems for several small values of p. For instance, we discovered that the square of any integer must take one of the forms $5k$, $5k + 1$ or $5k + 4$. That is, in arithmetic modulo 5, the squares are 0, 1 and 4. It follows that the quadratic congruences

$$x^2 \equiv 2 \pmod{5} \quad \text{and} \quad x^2 \equiv 3 \pmod{5}$$

are each unsolvable.

As the solution of quadratic equations presents little or no challenge, the thought of devoting a whole unit to quadratic congruences might well seem unexciting. Be patient! Investigation of when a quadratic congruence is solvable (without actually solving it) leads us through three of the outstanding results of number theory: Euler's Criterion, Gauss' Lemma and the Quadratic Reciprocity Law. The latter is a most fascinating result, described by Gauss as 'the gem of higher arithmetic'. The consequences of these results are far-reaching in other areas of number theory. In this unit we shall use them to establish some more particular cases of Dirichlet's Theorem (which we promised in *Unit 2*). There are numerous applications to the solution of Diophantine equations, some of which we shall meet in *Unit 8*.

The unit is based on Chapter 9 of **B**. Section 6.1 looks at Euler's Criterion, and introduces some new terminology. Section 6.2 presents the Legendre symbol (a most convenient shorthand for the new terminology) and investigates its properties. Section 6.3 proves Gauss' Lemma and numerous corollaries of it. Finally, Section 6.4 is concerned with the Quadratic Reciprocity Law and its applications, and is a tape-based section.

In Chapter 9 of **B** the author gives several alternative proofs of results whilst pursuing a subsidiary line involving primitive roots. As we have chosen to omit primitive roots from our course, we have to steer a careful path through the chapter.

6.1 Euler's Criterion

In this section we obtain a first test, known as Euler's Criterion, for deciding whether or not the congruence $x^2 \equiv a \pmod{p}$ has a solution. In real terms, Euler's Criterion is not a very practical method to employ when the prime p is large, but nevertheless the test will prove crucial for subsequent theoretical considerations.

We start, however, with a look at the problem of solving a general quadratic congruence, and introduce some new terminology.

READ B Section 9.1, page 184 as far as page 186, line 19.

NOTES (i) *Page 184, bottom*

The preceding argument has shown that the general quadratic congruence (1) is equivalent, after appropriate changes of variable, to congruence (2). The latter has solutions when the integer d is congruent to a 'square', modulo p. Therefore to solve the quadratic congruence we require a knowledge of which integers are 'the squares, modulo p'.

Notice that if y_0 is a solution of congruence (2), then to recover a solution of the equivalent congruence (1), via the equation $y = 2ax + b$, we have to solve the linear congruence $2ax \equiv y_0 - b \pmod{p}$. But since $\gcd(2a, p) = 1$, this congruence has a unique solution (Corollary, **B** page 84). The numerical example in Note (ii) will illustrate the various stages of this argument.

(ii) *Page 185, line 14*

In this numerical example, **B** has taken $a = 5$, $b = -6$, $c = 2$ and $p = 13$, and substituted these values into the various formulae on page 184. We shall look at the example in more detail. To solve the congruence $5x^2 - 6x + 2 \equiv 0 \pmod{13}$, we first multiply through by $4a = 20$ obtaining

$$100x^2 - 120x + 40 \equiv 0 \pmod{13}.$$

This allows us to 'complete the square':

$$(10x - 6)^2 + 4 \equiv 0 \pmod{13}.$$

Adding 9 to each side, this becomes

$$(10x - 6)^2 \equiv 9 \pmod{13}.$$

(At this stage in the accompanying theory we have $d = 9$ and we make the substitution $y = 10x - 6$.)

This gives two possibilities, namely

$$10x - 6 \equiv 3 \pmod{13} \quad \text{and} \quad 10x - 6 \equiv -3 \pmod{13}.$$

(Lagrange's Theorem shows that these two are the only possibilities.) These give

$$10x \equiv 9 \pmod{13} \quad \text{and} \quad 10x \equiv 3 \pmod{13}$$

and since $\gcd(10, 13) = 1$, these linear congruences have unique solutions, which are respectively

$$x \equiv 10 \pmod{13} \quad \text{and} \quad x \equiv 12 \pmod{13}. \quad \blacktriangle$$

So the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is solvable if and only if $b^2 - 4ac$ is a quadratic residue of p. If this is the case, then the method given on **B** page 184 (illustrated by the example in Note (ii)) will always lead systematically to the solutions. However, there are many other ways of solving quadratic congruences. For example, look again at the congruence

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}.$$

As a first step we can change the coefficients by multiplying through by any integer which is not a multiple of 13. Probably the simplest solution stems from multiplying by 8:

$$\begin{aligned} 40x^2 - 48x + 16 &\equiv x^2 + 4x + 3 \\ &\equiv (x + 2)^2 - 1 \equiv 0 \pmod{13}. \end{aligned}$$

Therefore $x + 2 \equiv \pm 1 \pmod{13}$, giving $x \equiv 10, 12 \pmod{13}$, as before.

We chose to multiply through by 8 simply because 8 is the multiplicative inverse modulo 13 of the coefficient 5 of x^2, and therefore it converts the quadratic congruence to an equivalent one where the coefficient of x^2 is 1. The advantage of this is illustrated by the ease with which we completed the above solution.

In our Solution to SAQ 1 we suggest various other ways of attacking quadratic congruences. There is also a point worth noting in the Solution to SAQ 2 about the number of quadratic residues of an odd prime p.

SAQ 1 **B** page 189, Problems 9.1, number 1.

SAQ 2 **B** page 189, Problems 9.1, number 2.

SOLUTION TO SAQ 1

(a) $$\begin{aligned} x^2 + 7x + 10 &\equiv x^2 + 18x + 10 \pmod{11} \quad (\text{since } 7 \equiv 18 \pmod{11}) \\ &\equiv (x+9)^2 - 71 \\ &\equiv (x+9)^2 - 5 \equiv 0 \pmod{11}. \end{aligned}$$

Therefore $(x+9)^2 \equiv 5 \equiv 16 \pmod{11}$, whence $x + 9 \equiv \pm 4 \pmod{11}$, giving $x \equiv 6 \pmod{11}$ or $x \equiv 9 \pmod{11}$.

Alternatively, the quadratic can be factorized:

$$x^2 + 7x + 10 = (x+5)(x+2) \equiv 0 \pmod{11}.$$

By Theorem 3-1 of **B** page 47, it follows that either $x + 5 \equiv 0 \pmod{11}$ or $x + 2 \equiv 0 \pmod{11}$, giving $x \equiv 6, 9 \pmod{11}$, as before.

(b) We first convert the coefficient of x^2 to 1. We can achieve this either by multiplying through by 9 or by cancelling common 3s:

$$\begin{aligned} 3x^2 + 9x + 7 &\equiv 3x^2 + 9x + 33 \pmod{13} \quad (\text{since } 7 \equiv 33 \pmod{13}) \\ &\equiv 3(x^2 + 3x + 11) \equiv 0 \pmod{13}. \end{aligned}$$

Since $13 \nmid 3$, this is equivalent to

$$\begin{aligned} x^2 + 3x + 11 &\equiv x^2 + 16x + 11 \\ &\equiv (x+8)^2 - 53 \\ &\equiv (x+8)^2 - 1 \equiv 0 \pmod{13}. \end{aligned}$$

Therefore $x + 8 \equiv \pm 1 \pmod{13}$, giving $x \equiv 4, 6 \pmod{13}$.

(c) Multiplying through by 14 (since $5 \cdot 14 \equiv 1 \pmod{23}$),

$$\begin{aligned} 70x^2 + 84x + 14 &\equiv x^2 - 8x + 14 \\ &\equiv (x-4)^2 - 2 \equiv 0 \pmod{23}. \end{aligned}$$

Therefore $(x-4)^2 \equiv 2 \equiv 25 \pmod{23}$, and so $x - 4 \equiv \pm 5 \pmod{23}$ giving $x \equiv 9, 22 \pmod{23}$.

Alternatively, the quadratic again factorizes:

$$5x^2 + 6x + 1 = (5x+1)(x+1) \equiv 0 \pmod{23}.$$

So either

$$x + 1 \equiv 0 \pmod{23} \iff x \equiv 22 \pmod{23}$$

or

$$5x + 1 \equiv 0 \pmod{23} \iff x \equiv 9 \pmod{23},$$

giving solutions $x \equiv 9, 22 \pmod{23}$. ■

SOLUTION TO SAQ 2

(a) In Example 9-1, we determined the quadratic residues of 13 by evaluating (modulo 13) the squares $1^2, 2^2, \ldots, 12^2$. In the same way, for any odd prime p, the quadratic residues of p are given by the squares $1^2, 2^2, \ldots, (p-1)^2$. However, since $r^2 = (-r)^2 \equiv (p-r)^2 \pmod{p}$, these $p - 1$ integers fall into congruent pairs modulo p, namely $1^2 \equiv (p-1)^2$, $2^2 \equiv (p-2)^2, \ldots,$ $\left(\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2$, and so a quadratic residue of p is congruent to one of $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

In fact, the integers listed above are incongruent modulo p, so that there are precisely $\frac{p-1}{2}$ quadratic residues of p. To see this, suppose $r^2 \equiv s^2 \pmod{p}$, where $1 \leq r, s \leq \frac{p-1}{2}$. This means that $p | r^2 - s^2$, and factorizing $r^2 - s^2 = (r-s)(r+s)$, Euclid's Lemma gives $p|(r+s)$ or $p|(r-s)$. Now $2 \leq r+s \leq p-1$, and so $p|r+s$ is impossible. Moreover, $|r-s| < \frac{p-1}{2}$ and so $p|r-s$ can occur only if $r=s$.

(b) From part (a), the quadratic residues of 17 are congruent modulo 17 to the squares of the first eight natural numbers:

$$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 9,\ 4^2 \equiv 16,\ 5^2 \equiv 8,\ 6^2 \equiv 2,\ 7^2 \equiv 15,\ 8^2 \equiv 13. \ \blacksquare$$

Before reading about Euler's Criterion, let us look at a couple of Examples.

EXAMPLE 1 In SAQ 2 (b), we saw that 3 is a quadratic nonresidue of 17. Consider the linear congruence $cx \equiv 3 \pmod{17}$, where c is any of the integers $1, 2, \ldots, 16$. Since $\gcd(c, 17) = 1$, this congruence has a unique solution. The solution is certainly not $x \equiv 0 \pmod{17}$, and neither is it $x \equiv c \pmod{17}$, for then $c^2 \equiv 3 \pmod{17}$ contradicts the fact that 3 is a quadratic nonresidue of 17. Hence, for each choice of c, the unique solution is one of the other integers in the set $\{1, 2, \ldots, 16\}$. It follows that these sixteen integers fall into eight pairs in such a way that the product of each pair is congruent to $3 \pmod{17}$. To be precise,

$$\begin{aligned} 1 \cdot 3 &\equiv 3 \pmod{17}, & 14 \cdot 16 &\equiv 3 \pmod{17}, \\ 2 \cdot 10 &\equiv 3 \pmod{17}, & 7 \cdot 15 &\equiv 3 \pmod{17}, \\ 4 \cdot 5 &\equiv 3 \pmod{17}, & 12 \cdot 13 &\equiv 3 \pmod{17}, \\ 6 \cdot 9 &\equiv 3 \pmod{17}, & 8 \cdot 11 &\equiv 3 \pmod{17}. \end{aligned}$$

Multiplying together these eight congruences, we obtain

$$16! \equiv 3^8 \pmod{17}.$$

But we know from Wilson's Theorem that $16! \equiv -1 \pmod{17}$, and so

$$3^8 \equiv -1 \pmod{17}.$$

The chosen integer 3 is not special in this example. If we select instead any other quadratic nonresidue of 17, say a, then we find that the sixteen integers from 1 to 16 inclusive fall into eight pairs whose product is congruent to $a \pmod{17}$. Multiplying together the resulting eight congruences gives

$$a^8 \equiv 16! \equiv -1 \pmod{17}.$$

What is more, we can replace 17 by any odd prime p and discover the following result.

If a is a quadratic nonresidue of p then $a^{(p-1)/2} \equiv -1 \pmod{p}$.

This is part of Euler's Criterion; the remaining part comes from a corresponding result when a is chosen to be a quadratic residue of p.

EXAMPLE 2 8 is a quadratic residue of 17. In SAQ 2 we found that the congruence $x^2 \equiv 8 \pmod{17}$ has two solutions: $x \equiv 5 \pmod{17}$ and $x \equiv 12 \pmod{17}$. If we ignore 5 and 12 then, just as in Example 1, the remaining fourteen integers in the set $\{1, 2, \ldots, 16\}$ fall into seven pairs whose product is congruent to 8 modulo 17:

$$\begin{array}{ll} 1 \cdot 8 \equiv 8 \pmod{17}, & 9 \cdot 16 \equiv 8 \pmod{17}, \\ 2 \cdot 4 \equiv 8 \pmod{17}, & 10 \cdot 11 \equiv 8 \pmod{17}, \\ 3 \cdot 14 \equiv 8 \pmod{17}, & 13 \cdot 15 \equiv 8 \pmod{17}. \\ 6 \cdot 7 \equiv 8 \pmod{17}, & \end{array}$$

If we multiply together the left-hand sides of these congruences, the outcome is not 16!, since the integers 5 and 12 are missing. To rectify this, and so that we can subsequently appeal to Wilson's Theorem, we include the additional congruence whose left-hand side is 5 times 12:

$$5 \cdot 12 \equiv 5 \cdot (-5) \equiv -5^2 \equiv -8 \pmod{17}.$$

(It is no accident that the right-hand side turns out to be the negative of the quadratic residue under consideration.)

Multiplying together all eight congruences, we have

$$16! \equiv 8^7 \cdot (-8) \equiv -8^8 \pmod{17}$$

and using Wilson's Theorem ($16! \equiv -1 \pmod{17}$), we arrive at

$$8^8 \equiv 1 \pmod{17}.$$

Again we can replace 17 by any odd prime p and 8 by any quadratic residue of p, say a, and the above argument generalizes to show

$$a^{(p-1)/2} \equiv 1 \pmod{p}. \quad \square$$

The proof of Euler's Criterion in the next reading passage consists of the generalizations of our two examples. The statement of Euler's Criterion in **B** is as follows:

a is a quadratic residue of the odd prime p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

We shall, however, prove the stronger formulation given as the Corollary on page 187.

READ B from the statement of the Corollary on page 187 to the end of Section 9.1.

EXAMPLE 3 **B** page 189, Problems 9.1, number 8 part (a).

When dealing with quadratic residues and nonresidues of p it is important to remember that we exclude from consideration the multiples of p. Here, since we are given that ab is a quadratic residue, it follows that $p \nmid a$ and $p \nmid b$, for otherwise $p \mid ab$, which is not the case. So neither a nor b is a multiple of p.

Applying Euler's Criterion to the identity

$$(ab)^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2}$$

we obtain the quadratic nature (residue or nonresidue) of ab in terms of that of a and b. For example, if a is a nonresidue and b a residue, then

$$a^{(p-1)/2} \equiv -1, \quad b^{(p-1)/2} \equiv 1 \quad \Rightarrow \quad (ab)^{(p-1)/2} \equiv -1 \pmod{p},$$

showing ab to be a nonresidue. Looking at the four possible cases, we draw up the following multiplication table:

×	residue	nonresidue
residue	residue	nonresidue
nonresidue	nonresidue	residue

which is determined essentially by the various products of 1 and -1.

The table answers the question: residues arise only as the product of two integers of the same quadratic nature.

SAQ 3 Determine whether 5 is a quadratic residue or nonresidue for each of the primes $p = 11$, 13, and 17.

SAQ 4 If a is a quadratic residue of the odd prime p, prove that $p - a$ is a quadratic residue of p if and only if $p \equiv 1 \pmod 4$.

SAQ 5 **B** page 190, Problems 9.1, number 8 part (b).

SAQ 6 Lagrange's Theorem tells us that each of the polynomial congruences $x^{(p-1)/2} - 1 \equiv 0 \pmod p$ and $x^{(p-1)/2} + 1 \equiv 0 \pmod p$ has at most $\dfrac{p-1}{2}$ incongruent solutions. However,

$$(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = x^{p-1} - 1 \equiv 0 \pmod p$$

has exactly $p - 1$ solutions, since $x^{p-1} \equiv 1 \pmod p$ for $x = 1, 2, \ldots, p-1$, by Fermat's Theorem.

By showing that each quadratic residue of p is a solution of $x^{(p-1)/2} - 1 \equiv 0 \pmod p$, use the above information to give an alternative proof of Euler's Criterion.

SOLUTION TO SAQ 3

$$5^{(11-1)/2} = 5^5 = (25)^2 \cdot 5 \equiv 3^2 \cdot 5 \equiv 45 \equiv 1 \pmod{11},$$

so 5 is a quadratic residue of 11.

$$5^{(13-1)/2} = 5^6 = 25^3 \equiv (-1)^3 \equiv -1 \pmod{13},$$

so 5 is a quadratic nonresidue of 13.

$$5^{(17-1)/2} = 5^8 = 25^4 \equiv 8^4 = 64^2 \equiv 13^2 \equiv 169 \equiv -1 \pmod{17},$$

so 5 is a quadratic nonresidue of 17. ■

SOLUTION TO SAQ 4 $p - a \equiv -a \pmod p$. Therefore

$$(p-a)^{(p-1)/2} \equiv (-a)^{(p-1)/2} = (-1)^{(p-1)/2} \cdot a^{(p-1)/2}$$
$$\equiv (-1)^{(p-1)/2} \pmod p,$$

since $a^{(p-1)/2} \equiv 1 \pmod p$ by Euler's Criterion, a being a quadratic residue.

If $p \equiv 1 \pmod 4$, say $p = 4k + 1$, then

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1,$$

in which case $p - a$ is a quadratic residue of p.

On the other hand, if $p \equiv 3 \pmod 4$, say $p = 4k + 3$, then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1,$$

so that $p - a$ is a quadratic nonresidue of p. ■

SOLUTION TO SAQ 5 Consider the congruence $ax^2 \equiv b \pmod p$, where a and b are of the same quadratic nature modulo p. Being either a quadratic residue or nonresidue, $a \not\equiv 0 \pmod p$ and so (as we have seen several times before, most recently in the proof of Euler's Criterion) a has a multiplicative inverse a', that is, an integer a' such that $aa' \equiv 1 \pmod{p}$. Now $1 = 1^2$ is certainly a residue of every prime. As the product aa' is a residue of p it follows from Example 3 that a' and a (and therefore b also) are of the same quadratic nature.

Multiplying through the given congruence by a' (obtaining an equivalent congruence since $\gcd(a', p) = 1$), we have

$$a'ax^2 \equiv x^2 \equiv a'b \pmod{p}.$$

But as a' and b are of the same quadratic nature, their product is known to be a residue, and so $x^2 \equiv a'b \pmod{p}$ certainly has a solution. ■

SOLUTION TO SAQ 6 From the information given, each of the polynomial congruences $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ and $x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$ has exactly $\frac{1}{2}(p-1)$ solutions. We have seen in the Solution to SAQ 2 that there are exactly $\frac{1}{2}(p-1)$ quadratic residues of p. If we can show that each of the $\frac{1}{2}(p-1)$ quadratic residues is a solution of $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$, it will follow that the remaining $\frac{1}{2}(p-1)$ non-zero least positive residues, which are the quadratic nonresidues, must each be a solution of $x^{(p-1)/2} + 1 \equiv 0 \pmod{p}$.

Let x be a quadratic residue of p. Then $x \equiv a^2 \pmod{p}$, for some integer a with $\gcd(a, p) = 1$. But then

$$x^{(p-1)/2} \equiv (a^2)^{(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod{p},$$

by Fermat's Theorem, and so $x^{(p-1)/2} - 1 \equiv 0 \pmod{p}$.

It follows that a is a quadratic residue or nonresidue of p if and only if, respectively,

$$a^{(p-1)/2} - 1 \equiv 0 \pmod{p} \quad \text{or} \quad a^{(p-1)/2} + 1 \equiv 0 \pmod{p}.$$

This is Euler's Criterion. ■

6.2 The Legendre Symbol

Throughout the previous section, you will have noticed the large number of times we wrote down statements such as 'a is a quadratic (non)residue of p'. You probably also noticed that from time to time we dropped the adjective 'quadratic' and referred simply to 'residues' and 'nonresidues'. It would be most convenient to have a shorthand notation for statements such as the above. To this end we shall introduce a very useful symbolism first used by Legendre.

The section pursues our investigation of properties of quadratic residues using the new notation.

READ B from the beginning of Section 9.2, page 190, as far as the statement of Theorem 9-4 on page 194.

NOTES (i) *Page 191, line −4*
The earlier example referred to is Example 9-1 on page 186.

(ii) *Page 192, line 16*
The proof given of Theorem 9-2 (1) is somewhat verbose. You might find the following argument clearer.

$$\begin{aligned}(a/p) = 1 &\Longleftrightarrow a \equiv x^2 \pmod{p}, \quad \text{for some integer } x\\ &\Longleftrightarrow b \equiv x^2 \pmod{p}, \quad \text{since } a \equiv b \pmod{p}\\ &\Longleftrightarrow (b/p) = 1.\end{aligned}$$

(iii) *Page 193, line 17*

In Example 9-4, the alert reader might spot that $-38 \equiv 1 \pmod{13}$, so that the congruence $x^2 \equiv -38 \pmod{13}$ has solutions $x \equiv \pm 1 \pmod{13}$. However, the example is intended to demonstrate parts of Theorem 9-2 in action and should be read in this spirit. The result itself is unimportant, but make sure you follow the steps taken in the argument.

(iv) *Page 194, line 14*

We proved Theorem 9-4 in our Solution to SAQ 2. There are $\frac{1}{2}(p-1)$ quadratic residues of p, and they are congruent modulo p to the squares $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. The remaining $\frac{1}{2}(p-1)$ incongruent numbers which are relatively prime to p are the quadratic nonresidues.

In the sum $\sum_{a=1}^{p-1} (a/p)$, we are counting $+1$ for each of the $\frac{1}{2}(p-1)$ residues and -1 for each of the $\frac{1}{2}(p-1)$ nonresidues. Clearly the total is zero. ▲

EXAMPLE 4 As an example of the use of the properties of Theorem 9-2, let us find all the quadratic residues of 37. We know that there are eighteen of them, and we could, of course, find them by evaluating $1^2, 2^2, \ldots, 18^2$ modulo 37, but we hope we can reduce the amount of computation.

For a start, we know that 1, 4, 9, 16, 25 and 36 are residues of 37 (this by (2)). As $36 \equiv -1 \pmod{37}$, (1) gives $(-1/37) = 1$, a fact that we could have established alternatively from (5). Using this together with (4) and (1),

$$1 = (-1/37)(4/37) = (-4/37) = (33/37),$$

showing that 33 is also a residue. In the same way, $-9 \equiv 28$, $-16 \equiv 21$ and $-25 \equiv 12$ are residues. Having found that 12 and 28 are residues we can bring property (6) into play:

$$1 = (12/37) = (2^2 \cdot 3/37) = (3/37)$$

and

$$1 = (28/37) = (2^2 \cdot 7/37) = (7/37).$$

So 3 and 7 are residues, as too are $-3 \equiv 34$ and $-7 \equiv 30$.

We have now found a total of 14 so there are four more outstanding. Using properties (4) and (1):

$$1 = (4/37)(12/37) = (48/37) = (11/37)$$

giving 11 and $-11 \equiv 26$ as two further residues.

Finally, using property (6) in a different way:

$$(3/37) = 1 \implies (3^2 \cdot 3/37) = (27/37) = 1$$

giving 27 and $-27 \equiv 10$ as the final two residues.

The complete list of residues of 37 is

$$1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.$$

SAQ 7 Using only the properties of Theorem 9-2, evaluate the following Legendre symbols.

(a) (3/11), (b) (19/17), (c) (40/11).

SAQ 8 Show that a is a quadratic residue of 31 if and only if $2a$ is also a quadratic residue. Use this fact to obtain all quadratic residues of 31.

SAQ 9 **B** page 203, Problems 9.2, number 12.

SOLUTION TO SAQ 7

(i)
$$\begin{aligned}(3/11) &= (3\cdot 2^2/11) && \text{(by (6))}\\ &= (12/11)\\ &= (1/11) && \text{(by (1))}\\ &= 1 && \text{(by (5))}\end{aligned}$$

(ii)
$$\begin{aligned}(19/17) &= (36/17) && \text{(by (1))}\\ &= 1 && \text{(by (2))}\end{aligned}$$

(iii)
$$\begin{aligned}(40/11) &= (4/11)(10/11) && \text{(by (4))}\\ &= (10/11) && \text{(by (2))}\\ &= (-1/11) && \text{(by (1))}\\ &= (-1)^5 && \text{(by (5))}\\ &= -1 \quad ■\end{aligned}$$

SOLUTION TO SAQ 8

$$\begin{aligned}(a/31) &= (8^2a/31) && \text{(by (6))}\\ &= (64a/31)\\ &= (2a/31) && \text{(by (1))}\end{aligned}$$

So if we double (modulo 31) any residue of 31 the outcome is another residue. Starting from residue 1, doubling gives further residues 2, 4, 8 and 16. Starting from $9 = 3^2$, doubling gives 18, $36 \equiv 5$, 10 and 20. Starting from $25 = 5^2$, doubling gives $50 \equiv 19$, $38 \equiv 7$, 14 and 28. We have now found fifteen residues, the correct number for the prime 31. They are

$$1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28. \quad ■$$

SOLUTION TO SAQ 9

In the sum $\sum_{a=1}^{(p-1)/2} (a/p)$, we are examining the set of integers $\{1, 2, \ldots, \frac{1}{2}(p-1)\}$ and counting 1 for each residue and -1 for each nonresidue. The total will be zero provided there are the same number of residues as nonresidues in this set.

In SAQ 4, we showed that if $p \equiv 1 \pmod 4$ then $(a/p) = (p - a/p)$. Hence if a is a residue in $\{1, 2, \ldots, \frac{1}{2}(p-1)\}$ then $p - a$ is a residue in $\{\frac{1}{2}(p+1), \ldots, p-1\}$, from which it follows that exactly one half of the residues are to be found in $\{1, 2, \ldots, \frac{1}{2}(p-1)\}$. This set therefore contains $\frac{1}{4}(p-1)$ residues and $\frac{1}{4}(p-1)$ nonresidues. ■

6.3 Gauss' Lemma

In this section we shall prove Gauss' Lemma and look at some consequences. Gauss' Lemma gives another test for whether or not an integer is a quadratic residue of a prime, and, like Euler's Criterion, whilst not being a very practicable test when large numbers are involved, it is an important theoretical result.

Before embarking on a proof of Gauss' Lemma we shall look at an example which should clarify the statement of the result and, more important, will illustrate the line to be adopted in the general proof.

READ B the statement of Gauss' Lemma, Theorem 9-5 on page 195.

EXAMPLE 5 Let $p = 19$ and $a = 11$. The set S in Gauss' Lemma consists of the first $\frac{1}{2}(p-1) = 9$ multiples of 11:

$$S = \{11, 22, 33, 44, 55, 66, 77, 88, 99\}.$$

Replacing each member of S by its remainder on division by 19, that is, by the least positive residue of 19 to which it is congruent, we get

$$S' = \{11, 3, 14, 6, 17, 9, 1, 12, 4\}.$$

There are five members of S' which are less than $\frac{1}{2}p$ and four members, namely 11, 14, 17 and 12, which exceed $\frac{1}{2}p$. Hence, according to Gauss' Lemma,

$$(11/19) = (-1)^4 = 1$$

and 11 is a quadratic residue of 19.

Suppose now that we replace the four members of S' which exceed $\frac{1}{2}p$ by their negatives, achieved up to congruence by subtraction from 19. This results in the new set

$$S'' = \{8, 3, 5, 6, 2, 9, 1, 7, 4\}.$$

Notice that S'' consists of the first nine natural numbers. This is no accident! The crux of the proof of Gauss' Lemma lies in showing that, for any prime p and relatively prime integer a, the set S'', constructed from multiples of a in this way, consists of the first $\frac{1}{2}(p - 1)$ natural numbers. It is a short step from here to completion of the proof.

Returning to our specific example, notice that the product of the elements in S'' is $9!$, whilst the product of the elements in S is $11^9 \cdot 9!$ Now corresponding elements of the sets S and S'' are congruent modulo 19, with the exception of the four sign changes involved in getting from S' to S''. It follows that

$$11^9 \cdot 9! \equiv (-1)^4 9! \pmod{19}$$

giving

$$11^9 \equiv 1 \pmod{19}, \quad \text{since } \gcd(19, 9!) = 1.$$

Euler's Criterion now confirms that 11 is a quadratic residue of 19.

The proof of Gauss' Lemma retraces this example in generality, for arbitrary odd prime p and any integer a with $\gcd(a, p) = 1$.

READ B page 195, line -7 to page 198, line -7.

NOTES (i) *Page 195, bottom*
The set of residues $\{r_1, r_2, \ldots, r_m, s_1, \ldots, s_n\}$ corresponds to the set S' of Example 5 (although the members are presented in a different order). $\{r_1, r_2, \ldots, r_m, p - s_1, \ldots, p - s_n\}$ corresponds to our set S''.

(ii) *Page 196, line 15*
The use of square brackets here, and two further instances in the next eight lines, is accidental. They do *not* denote the greatest integer function.

(iii) *Page 198, top*
We have found that the number of integers in the set $\{2, 4, 6, \ldots, p - 1\}$ which exceed $\frac{1}{2}p$ is $\frac{1}{2}(p - 1) - [\frac{1}{4}p]$. To apply Gauss' Lemma we need to raise -1 to this power, and so what we really need to know now is whether $\frac{1}{2}(p - 1) - [\frac{1}{4}p]$ is even or odd. To achieve this we have to look at the four forms for an odd prime modulo 8. It is not good enough, for instance, to work with the two forms $4k + 1$ and $4k + 3$, for if $p = 4k + 1$ then

$$\tfrac{1}{2}(p - 1) - [\tfrac{1}{4}p] = 2k - [k + \tfrac{1}{4}] = k$$

and this can still be either even or odd. ▲

SAQ 10 **B** page 201, Problems 9.2, number 1 parts (a), (c) and (e).

SAQ 11 **B** page 202, Problems 9.2, numbers 4 and 5.

SAQ 12 **B** page 209, Problems 9.3, number 4.

SOLUTION TO SAQ 10

As in the proof of Gauss' Lemma, to determine (a/p) we form the set S consisting of the first $\frac{1}{2}(p-1)$ positive multiples of a, reduce each to its least positive residue modulo p, and count how many resulting members exceed $p/2$. This gives the number n in Gauss' Lemma.

(a) $a = 8, p = 11.$

$$S = \{8, 16, 24, 32, 40\} \equiv \{\underline{8}, 5, 2, \underline{10}, \underline{7}\}.$$

$$n = 3, \quad \text{so } (8/11) = (-1)^3 = -1.$$

(c) $a = 5, p = 19.$

$$S = \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$$

$$\equiv \{5, \underline{10}, \underline{15}, 1, 6, \underline{11}, \underline{16}, 2, 7\}.$$

$$n = 4, \quad \text{so } (5/19) = (-1)^4 = +1.$$

(e) $a = 6, p = 31.$

$$S = \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90\}$$

$$\equiv \{6, 12, \underline{18}, \underline{24}, \underline{30}, 5, 11, \underline{17}, \underline{23}, \underline{29}, 4, 10, \underline{16}, \underline{22}, \underline{28}\}.$$

$$n = 9, \quad \text{so } (6/31) = (-1)^9 = -1. \quad ■$$

SOLUTION TO SAQ 11

4. By Theorem 9-6, $(2/p) = 1$ for $p \equiv 7 \pmod 8$. By Theorem 9-2 (3), $(2/p) \equiv 2^{(p-1)/2} \pmod p$. Combining these results gives, for $p \equiv 7 \pmod 8$, $2^{(p-1)/2} \equiv 1 \pmod p$, or $p | 2^{(p-1)/2} - 1$.

5. The numbers in question, $M_n = 2^n - 1$, are the Mersenne numbers which we mentioned in *Unit* 5. If n is composite, M_n is known to be composite, but for p prime M_p might or might not be prime. The above result uncovers many composite values of M_p, for it tells us that if $p \equiv 7 \pmod 8$ is a prime such that $\frac{1}{2}(p-1)$ is also prime, then $M_{(p-1)/2}$ is composite (being divisible by p).

   For $p = 23$, $\frac{1}{2}(p-1) = 11$ is also prime and so $23 | M_{11}$.

   Similarly, M_{23}, M_{83}, M_{131}, M_{179}, M_{183}, M_{239} and M_{251} are shown to be composite by applying the above result to the respective primes 47, 167, 263, 359, 367, 479 and 503. ■

SOLUTION TO SAQ 12

To apply Gauss' Lemma we look at the set

$$S = \{-2, -4, -6, \ldots, -(p-1)\}.$$

Adding p to each member of S (and reversing the order), we obtain the congruent set, which are positive least residues:

$$S' = \{1, 3, 5, \ldots, p-4, p-2\}.$$

We need to count how many of these integers exceed $p/2$. To do this we look separately at the four possible forms of p modulo 8.

(i) If $p = 8k + 1$, then the members of S' which exceed $p/2$ are

$$4k + 1, 4k + 3, \ldots, 8k - 1,$$

of which there are $2k$. In this case, $(-2/p) = (-1)^{2k} = 1$.

(ii) If $p = 8k + 3$, then the corresponding list is

$$4k + 3, 4k + 5, \ldots, 8k + 1,$$

of which there are again $2k$, giving $(-2/p) = 1$.

(iii) If $p = 8k + 5$, the list is

$$4k + 3, 4k + 5, \ldots, 8k + 3,$$

of which there are $2k + 1$. In this case $(-2/p) = (-1)^{2k+1} = -1$.

(iv) If $p = 8k + 7$, the list is

$$4k + 5, 4k + 7, \ldots, 8k + 5,$$

of which there are again $2k + 1$, giving $(-2/p) = -1$.

Alternatively

$$\begin{aligned}(-2/p) &= (-1/p) \cdot (2/p) \qquad \text{(by Theorem 9-2 (4))}\\ &= (-1)^{(p-1)/2} \cdot (-1)^{(p^2-1)/8} \qquad \text{(by Theorems 9-2 (5) and 9-6 (Corollary))}\\ &= (-1)^{((p-1)/2)+((p^2-1)/8)}\\ &= (-1)^{(p^2+4p-5)/8}.\end{aligned}$$

Therefore $(-2/p) = 1$, provided $p^2 + 4p - 5 \equiv 0 \pmod{16}$, which is the case when $p = 8k + 1$ or $p = 8k + 3$. On the other hand, $(-2/p) = -1$ provided $p^2 + 4p - 5 \equiv 8 \pmod{16}$, which is the case when $p = 8k + 5$ or $p = 8k + 7$. ■

READ B page 199, line −6 to page 200, line 8.

NOTE *Page 200, line 5*

$$N = (4p_1p_2 \cdots p_n)^2 - 2 = 2\{2(2p_1p_2 \cdots p_n)^2 - 1\}.$$

As the expression in curly brackets is odd, N is equal to twice a product of odd primes. If each of these odd prime divisors of N were congruent to 1 modulo 8, then so too would be their product, forcing $N = 2(8a + 1) = 16a + 2$. This cannot be the case since N is of the form $16a - 2$. ▲

SAQ 13 For any given integer $n \geq 2$, let $N = 2(n!)^2 - 1$, and let p be a prime divisor of N. By actually finding a solution of the congruence $x^2 \equiv 2 \pmod{p}$, show that $(2/p) = 1$. Hence, using Theorem 9-6, deduce that N must have a prime divisor of the form $8k + 7$.

Why does this argument prove that there are infinitely many primes of the form $8k + 7$?

SOLUTION TO SAQ 13 If p is a prime divisor of $N = 2(n!)^2 - 1$, then p is odd and $2(n!)^2 \equiv 1 \pmod{p}$. Multiplying by 2 gives $(2(n!))^2 \equiv 2 \pmod{p}$, showing that $(2/p) = 1$. According to Theorem 9-6, either $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$.

Now, if every prime divisor of N is of the form $8k + 1$, then so is N. But N is of the form $8k - 1$ (since $8 | 2(n!)^2$, for $n \geq 2$). Therefore N must have at least one prime divisor of the form $8k + 7$.

Suppose there are only finitely many primes of the form $8k + 7$, and let n be the largest of them. Then $2(n!)^2 - 1$ is divisible by a prime $p = 8k + 7$ and, as $p \leq n$, $p | n!$ Therefore $p | 2(n!)^2$. This is a clear contradiction since it forces $p | 1$. ■

6.4 Quadratic Reciprocity

We now turn to what is undisputably one of the most fascinating results in the whole of mathematics—Gauss' Quadratic Reciprocity Law. Amongst its numerous applications, the law provides us with yet another test for when an integer a is a quadratic residue of a prime, but, unlike its predecessors, this test is simple to employ even when the integers in question are very large.

As you have already read, there are many different proofs of the Quadratic Reciprocity Law. We have elected to present here our favourite proof, which is slightly different from the proof given in **B**. If you wish to study the proof in **B**, either instead of or in addition to our proof, then you will need to read first the Lemma on **B** pages 200 and 201.

READ B Section 9.3, page 203, as far as the statement of the Quadratic Reciprocity Law on page 204.

START THE TAPE WHEN YOU ARE READY

FRAME 1 Gauss' Quadratic Reciprocity Law

If p and q are distinct odd primes then

$$(p/q)\cdot(q/p) = (-1)^{(p-1)(q-1)/4},$$

that is

$$\begin{aligned} (p/q) &= (q/p) && \text{if either } p \text{ or } q \text{ is congruent to 1 modulo 4} \\ (p/q) &= -(q/p) && \text{if } p \equiv q \equiv 3 \pmod 4. \end{aligned}$$

FRAME 2 Example 6

Is 31 a quadratic residue of 73?

$$\begin{aligned} (31/73) &= (73/31), && \text{since } 73 \equiv 1 \pmod 4 \\ &= (11/31), && \text{since } 73 \equiv 11 \pmod{31} \\ &= -(31/11), && \text{since } 11 \equiv 31 \equiv 3 \pmod 4 \\ &= -(9/11), && \text{since } 31 \equiv 9 \pmod{11} \\ &= -1, && \text{since } (9/11) = (3^2/11) = 1. \end{aligned}$$

FRAME 3 Restating the problem via Gauss' Lemma

Let m be the number of integers in the set

$$\{q, 2q, \ldots, \tfrac{1}{2}(p-1)q\}$$

which have least positive residue modulo p exceeding $p/2$.

Let n be the number of integers in the set

$$\{p, 2p, \ldots, \tfrac{1}{2}(q-1)p\}$$

which have least positive residue modulo q exceeding $q/2$.

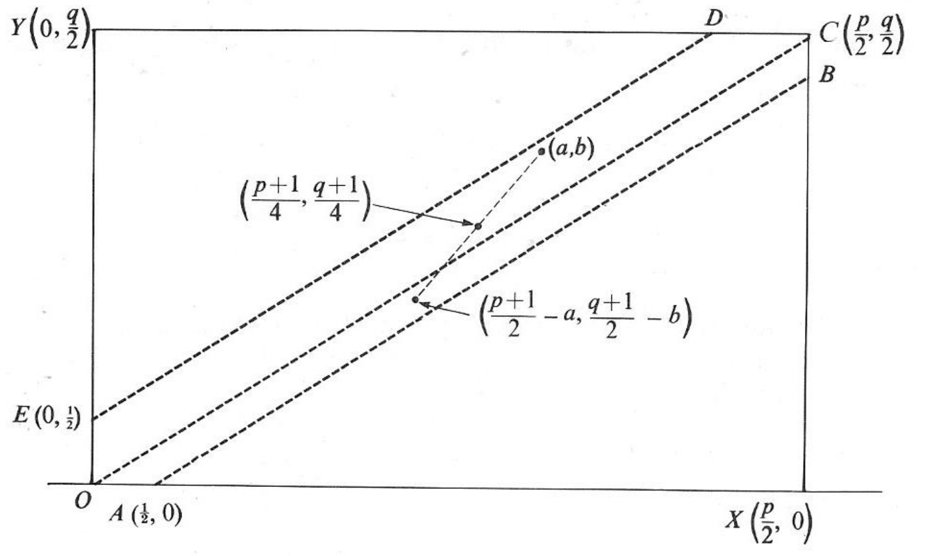
Gauss' Lemma: $(q/p) = (-1)^m$; $(p/q) = (-1)^n$.

Now $(p/q) = (q/p) \Longleftrightarrow (p/q)\cdot(q/p) = (-1)^{m+n} = 1$.

So to prove the Quadratic Reciprocity Law:

Show that $m + n$ is even except when $p \equiv q \equiv 3 \pmod 4$.

FRAME 4 Diagram


$Y\left(0,\frac{q}{2}\right)$
D
$C\left(\frac{p}{2},\frac{q}{2}\right)$
B
(a,b)
$\left(\frac{p+1}{4},\frac{q+1}{4}\right)$
$\left(\frac{p+1}{2}-a,\frac{q+1}{2}-b\right)$
$E\left(0,\frac{1}{2}\right)$
O
$A\left(\frac{1}{2},0\right)$
$X\left(\frac{p}{2},0\right)$

$OXCY$ is the rectangle with vertices $(0,0)$, $(p/2,0)$, $(p/2,q/2)$ and $(0,q/2)$, respectively.

OC is a diagonal and AB and ED are parallel to OC passing respectively through $(\frac{1}{2},0)$ and $(0,\frac{1}{2})$.

Equations:

$$OC:\quad y=\frac{q}{p}x, \qquad AB:\quad y=\frac{q}{p}(x-\tfrac{1}{2}), \qquad ED:\quad y=\frac{q}{p}x+\tfrac{1}{2}.$$

FRAME 5 Plan of the proof

Lattice points in $OXCY$ are points with coordinates (a,b) where a and b are both positive integers.

We shall show:

(1) The number of lattice points inside the hexagon $OABCDE$ is even, except when $p\equiv q\equiv 3 \pmod 4$.

(2) The number of lattice points in quadrilateral $OABC$ is n.

(3) The number of lattice points in quadrilateral $OCDE$ is m.

(4) None of the lattice points inside $OABCDE$ lie on OC.

FRAME 6 Outline proof of (1)

The lattice points in $OABCDE$ fall naturally into pairs, because if (a,b) is such a point, then so too is $\left(\frac{p+1}{2}-a,\frac{q+1}{2}-b\right)$. These points are on the straight line through, and equidistant from, the point $\left(\frac{p+1}{4},\frac{q+1}{4}\right)$. (See Frame 4.)

There is one exception to this pairing. (a,b) and $\left(\frac{p+1}{2}-a,\frac{q+1}{2}-b\right)$ are the same point when $a=\frac{p+1}{4}$ and $b=\frac{q+1}{4}$. Hence, if $\left(\frac{p+1}{4},\frac{q+1}{4}\right)$ is a lattice point, which will be the case precisely when $p\equiv q\equiv 3 \pmod 4$, this exceptional point is paired with itself. In this case alone the total number of lattice points in $OABCDE$ will be odd.

FRAME 7 Detailed proof of (1)

The interior of the hexagon $OABCDE$ consists of points (x, y) satisfying the constraints

$$0 < x < \frac{p}{2};\quad 0 < y < \frac{q}{2};$$

$$y < \frac{q}{p}x + \frac{1}{2};\quad y > \frac{q}{p}x - \frac{q}{2p}. \qquad \text{(See Frame 4.)}$$

It is our contention that if $x = a$, $y = b$ satisfies these inequalities then so too does $x = \frac{p+1}{2} - a$, $y = \frac{q+1}{2} - b$.

$$0 < a < \frac{p}{2} \Rightarrow \frac{1}{2} < \frac{p+1}{2} - a < \frac{p+1}{2}$$

$$\Rightarrow 0 < \frac{p+1}{2} - a < \frac{p}{2}$$

$$\left(\text{since } \frac{p+1}{2} - a \text{ is an integer}\right).$$

Similarly,

$$0 < b < \frac{q}{2} \Rightarrow \frac{1}{2} < \frac{q+1}{2} - b < \frac{q+1}{2}$$

$$\Rightarrow 0 < \frac{q+1}{2} - b < \frac{q}{2}.$$

$$b > \frac{q}{p}a - \frac{q}{2p} \Rightarrow -b < \frac{q}{2p} - \frac{q}{p}a$$

$$\Rightarrow \frac{q+1}{2} - b < \frac{q+1}{2} + \frac{q}{2p} - \frac{q}{p}a$$

$$= \frac{q}{p}\left(\frac{p+1}{2} - a\right) + \frac{1}{2},$$

and

$$b < \frac{q}{p}a + \frac{1}{2} \Rightarrow \frac{q+1}{2} - b > \frac{q+1}{2} - \frac{q}{p}a - \frac{1}{2}$$

$$= \frac{q}{p}\left(\frac{p+1}{2} - a\right) - \frac{q}{2p}. \quad \blacksquare$$

FRAME 8 Proof of (2)

Objective: To show there is a one-one correspondence between the lattice points in $OABC$ and the numbers in the set $\{p, 2p, 3p, \ldots, \frac{q-1}{2}p\}$ which have least positive residue modulo q exceeding $\frac{q}{2}$.

If (a, b) is a lattice point in $OABC$ then

$$\frac{q}{p}a - \frac{q}{2p} < b < \frac{q}{p}a \qquad \text{(i)}$$

and

$$0 < b < \frac{q}{2}. \qquad \text{(ii)}$$

Multiplying (i) by p and adding $q - qa$ gives

$$\frac{q}{2} < bp - q(a-1) < q. \qquad \text{(iii)}$$

Now $bp \equiv bp - q(a-1) \pmod{q}$, and so (iii) says that bp has least positive residue modulo q exceeding $\frac{q}{2}$.

The argument reverses. Choosing b from the set $\left\{1, 2, 3, \ldots, \frac{q-1}{2}\right\}$ (so that (ii) holds), if bp has least positive residue modulo q exceeding $\frac{q}{2}$ then there exists an integer a such that (iii), and hence (i) holds. (a, b) is therefore a lattice point in $OABC$. ■

FRAME 9 Proof of (3)

The proof of (3) is almost identical to the proof of (2), with the roles of p and q interchanged.

SAQ 14

Prove (3).

FRAME 9A Solution to SAQ 14

If (a, b) is a lattice point in $OCDE$ then

$$\frac{q}{p}a < b < \frac{q}{p}a + \frac{1}{2} \qquad \text{(i)}$$

and

$$0 < a < \frac{p}{2}. \qquad \text{(ii)}$$

Multiplying (i) by $-p$ gives

$$-qa > -bp > -qa - \frac{p}{2}$$

and adding $qa + p$ gives

$$p > qa - (b-1)p > \frac{p}{2}. \qquad \text{(iii)}$$

(iii) shows that qa has least positive residue modulo p exceeding $p/2$.

Conversely, if a is chosen from the set $\left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$ so that aq has least positive residue modulo p exceeding $\frac{p}{2}$, then there is an integer b such that (iii), and equivalently (i), holds. (a, b) is then a lattice point in $OCDE$. ■

FRAME 10 Proof of (4)

If (a, b) is a lattice point on OC then $b = \frac{q}{p}a$. Hence $p|qa$, and since $\gcd(p, q) = 1$, $p|a$. Inside $OABCDE$ we have $0 < a < \frac{p}{2}$, and so $p|a$ is impossible. ■

FRAME 11 **Example 7**

Does the quadratic congruence

$$3x^2 - 8x - 5 \equiv 0 \pmod{139}$$

have any solutions?

$$b^2 - 4ac = (-8)^2 - 4 \cdot 3 \cdot (-5) = 124$$

The congruence has solutions provided that 124 is a quadratic residue of 139.

$$\begin{aligned}
(124/139) &= (4/139) \cdot (31/139) \\
&= 1 \cdot (31/139) && (\text{since } 4 = 2^2) \\
&= -(139/31) && (\text{since } 139 \equiv 31 \equiv 3 \pmod{4}) \\
&= -(15/31) && (\text{since } 139 \equiv 15 \pmod{31}) \\
&= -(3/31)(5/31) \\
&= (31/3)(5/31) && (\text{since } 31 \equiv 3 \pmod{4}) \\
&= (31/3)(31/5) && (\text{since } 5 \equiv 1 \pmod{4}) \\
&= (1/3)(1/5) \\
&= 1.
\end{aligned}$$

The congruence has solutions.

FRAME 12 For more examples,

READ B from page 206, line -10 as far as the end of Example 9-6 on page 208.

END OF TAPE

SAQ 15 (a) Evaluate the following Legendre symbols:

(i) $(-219/383)$, (ii) $(461/773)$.

(383, 461 and 773 are primes.)

(b) Are the following congruences solvable?

(i) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$

(ii) $2x^2 + 5x - 9 \equiv 0 \pmod{1111}$.

SAQ 16 If p and q are distinct odd primes, prove that $(-p/q) = (-q/p)$ if and only if $p \equiv q \equiv 1 \pmod{4}$.

SAQ 17 **B** page 209, Problems 9.3, number 5.

SAQ 18 **B** page 210, Problems 9.3, number 8.

SOLUTION TO SAQ 15 (a) Explanations of the steps refer to properties (1), (2), (4) and (5) of the Legendre symbol (Theorem 9-2), Theorem 9-9 (GQRL) and Theorem 9-6.

(i)
$$\begin{aligned}
(-219/383) &= (164/383) && (\text{by } (1)) \\
&= (4/383) \cdot (41/383) && (\text{by } (4)) \\
&= 1 \cdot (383/41) && (\text{by } (2) \text{ and GQRL}) \\
&= (14/41) = (2/41) \cdot (7/41) && (\text{by } (1) \text{ and } (4))
\end{aligned}$$

$$\begin{aligned}
&= 1\cdot(7/41) && \text{(by 9-6)}\\
&= (41/7) && \text{(by GQRL)}\\
&= (6/7) = (2/7)\cdot(3/7) && \text{(by (1) and (4))}\\
&= 1\cdot(3/7) && \text{(by (9-6)}\\
&= -(7/3) && \text{(by GQRL: note } 7 \equiv 3 \,(\mathrm{mod}\, 4))\\
&= -(1/3) = -1. && \text{(by (1) and (5))}
\end{aligned}$$

(ii)
$$\begin{aligned}
(461/773) &= (773/461) = (312/461) && \text{(by GQRL and (1))}\\
&= (4/461)\cdot(2/461)\cdot(3/461)\cdot(13/461) && (312 = 2^3\cdot 3\cdot 13)\\
&= 1\cdot -1\cdot(461/3)\cdot(461/13) && \text{(by (2), 9-6 and GQRL)}\\
&= -1\cdot(2/3)\cdot(6/13) && \text{(by (1))}\\
&= -1\cdot -1\cdot(2/13)\cdot(3/13) && \text{(by 9-6 and (4))}\\
&= -1\cdot(3/13) &&\\
&= -(13/3) = -(1/3) = -1. && \text{(by GQRL and (1))}
\end{aligned}$$

(b) (i) $3x^2 + 6x + 5 \equiv 0 \,(\mathrm{mod}\, 89)$ is solvable provided $6^2 - 4\cdot 3\cdot 5 = -24$ is a quadratic residue of 89.

$$\begin{aligned}
(-24/89) &= (65/89) = (5/89)\cdot(13/89)\\
&= (89/5)\cdot(89/13)\\
&= (4/5)\cdot(11/13)\\
&= (13/11) = (2/11) = -1 \quad \Rightarrow \quad \text{No solutions.}
\end{aligned}$$

(ii) $1111 = 11\cdot 101$, and so the congruence $2x^2 + 5x - 9 \equiv 0 \,(\mathrm{mod}\, 1111)$ is solvable if and only if both the congruences $2x^2 + 5x - 9 \equiv 0 \,(\mathrm{mod}\, 11)$ and $2x^2 + 5x - 9 \equiv 0 \,(\mathrm{mod}\, 101)$ are solvable. This will be the case if $5^2 - 4\cdot 2\cdot(-9) = 97$ is a quadratic residue of both 11 and 101.

$$(97/11) = (9/11) = (3^2/11) = 1$$

$$(97/101) = (101/97) = (4/97) = (2^2/97) = 1$$

So the congruence has solutions. ■

SOLUTION TO SAQ 16

$$(-p/q) = (-1/q)(p/q) = (-1)^{\frac{1}{2}(q-1)}(p/q) \qquad \text{(by Theorem 9-2 (5))}$$

and

$$(-q/p) = (-1/p)(q/p) = (-1)^{\frac{1}{2}(p-1)}(q/p).$$

Therefore $(-p/q) = (-q/p)$ if either

(i) $(-1)^{\frac{1}{2}(q-1)} = (-1)^{\frac{1}{2}(p-1)}$ and $(p/q) = (q/p)$, or

(ii) $(-1)^{\frac{1}{2}(q-1)} = -(-1)^{\frac{1}{2}(p-1)}$ and $(p/q) = -(q/p)$.

Taking case (i), $(-1)^{\frac{1}{2}(q-1)} = (-1)^{\frac{1}{2}(p-1)}$ when $p \equiv q \,(\mathrm{mod}\, 4)$, whilst $(p/q) = (q/p)$ except when $p \equiv q \equiv 3 \,(\mathrm{mod}\, 4)$. We are left with the single solution $p \equiv q \equiv 1 \,(\mathrm{mod}\, 4)$.

Turning to (ii), $(p/q) = -(q/p)$ only when $p \equiv q \equiv 3 \,(\mathrm{mod}\, 4)$, but this possibility contradicts $(-1)^{\frac{1}{2}(q-1)} = -(-1)^{\frac{1}{2}(p-1)}$.

We conclude that $(-p/q) = (-q/p)$ if and only if $p \equiv q \equiv 1 \,(\mathrm{mod}\, 4)$. ■

SOLUTION TO SAQ 17

(a) $$(-3/p) = (-1/p)\cdot(3/p)$$

$$= \begin{cases} 1\cdot(p/3) & \text{if } p \equiv 1 \pmod 4 \\ -1\cdot -1\cdot(p/3) & \text{if } p \equiv 3 \pmod 4 \end{cases} \qquad \text{(by Theorem 9-2 (5) and GQRL)}$$

$$= (p/3)$$

$$= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

COMMENT This is the same as the given answer, for since a number of the form $6k + 4$ is not prime, the set of primes which are congruent to 1 modulo 3 is precisely the set of primes which are congruent to 1 modulo 6. Similarly, if p is a prime, then $p \equiv 2 \pmod 3$ if and only if $p \equiv 5 \pmod 6$. The result of (b) also shows that there are infinitely many primes of the form $3k + 1$.

(b) Suppose $p_1, p_2, \ldots, p_r$ are the only primes of form $6k + 1$ and consider $N = (2p_1p_2\cdots p_r)^2 + 3$.
As N is odd it has an odd prime divisor, say p. Then $(2p_1p_2 \ldots p_r)^2 \equiv -3 \pmod p$, from which $(-3/p) = 1$ and so $p \equiv 1 \pmod 6$ by part (a). But this means that p must be one of $p_1, p_2, \ldots, p_r$, whence $p|N$ and $p|(2p_1p_2 \ldots p_r)^2$, giving $p|3$. This implies that $p = 3$, contradicting $p \equiv 1 \pmod 6$. Hence there are infinitely many primes of the form $6k + 1$. ■

SOLUTION TO SAQ 18

(a) $(5/p) = (p/5)$. The quadratic residues of 5 are 1 and 4, so

$$(5/p) = 1 \iff p \equiv 1 \text{ or } 4 \pmod 5.$$

COMMENT Again this is a more compact form of the answer given in **B**.

(b) $(6/p) = (2/p)\cdot(3/p)$, so

$$(6/p) = 1 \iff \begin{cases} (2/p) = (3/p) = 1 \\ \text{OR} \\ (2/p) = (3/p) = -1 \end{cases}$$

$$\iff \begin{cases} p \equiv \pm 1 \pmod 8 \quad \text{AND} \quad p \equiv \pm 1 \pmod{12} \\ \text{OR} \\ p \equiv \pm 3 \pmod 8 \quad \text{AND} \quad p \equiv \pm 5 \pmod{12} \end{cases}$$

$$\iff \begin{cases} p \equiv 1 \text{ or } 23 \pmod{24} \\ \text{OR} \\ p \equiv 5 \text{ or } 19 \pmod{24} \end{cases}$$

$$\iff p \equiv 1, 5, 19 \text{ or } 23 \pmod{24}.$$

(c) $$(7/p) = \begin{cases} (p/7) & \text{if } p \equiv 1 \pmod 4 \\ -(p/7) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

The quadratic residues of 7 are 1, 2 and 4, hence

$$(7/p) = 1 \iff \begin{cases} p \equiv 1 \pmod 4 \quad \text{AND} \quad p \equiv 1, 2 \text{ or } 4 \pmod 7 \\ \text{OR} \\ p \equiv 3 \pmod 4 \quad \text{AND} \quad p \equiv 3, 5 \text{ or } 6 \pmod 7 \end{cases}$$

$$\iff \begin{cases} p \equiv 1, 9 \text{ or } 25 \pmod{28} \\ \text{OR} \\ p \equiv 3, 19 \text{ or } 27 \pmod{28} \end{cases}$$

$$\iff p \equiv 1, 3, 9, 19, 25 \text{ or } 27 \pmod{28}. \quad ■$$

6.5 Summary

The central theme of this unit concerns the problem of determining whether or not a quadratic congruence with prime modulus has solutions. The answer to this problem hinges around our ability to decide whether a given integer is a quadratic residue (i.e. congruent to a square) or nonresidue of the prime modulus.

In Section 6.1 we began our investigation of quadratic residues and showed that an odd prime p has $\frac{1}{2}(p-1)$ residues and $\frac{1}{2}(p-1)$ nonresidues. We obtained a first general test for residues, Euler's Criterion, which says that a is a quadratic residue of p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Section 6.2 pursued the development of the theory of quadratic residues, incorporating a new notation—the Legendre symbol:

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Theorem 9-2 (**B** page 192) contains the important properties of the Legendre symbol.

In Section 6.3 we gave a proof of Gauss' Lemma (**B** page 195), which is another test for the quadratic nature of an integer modulo p. Amongst several applications of Gauss' Lemma we proved some more special cases of Dirichlet's Theorem, that certain arithmetic progressions contain infinitely many primes.

The climax of the unit was Gauss' Quadratic Reciprocity Law (**B** page 204), which we proved in Section 6.4. This result, coupled with properties of the Legendre symbol, provides us with a relatively simple technique for deciding the solvability of any quadratic congruence with prime modulus.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 7
CONTINUED FRACTIONS

7.0 Introduction

The most obvious way of solving the quadratic equation $x^2 - x - 1 = 0$ is to use the well-known formula. Suppose, however, that we decide to solve the equation using an iterative method. The equation can be rearranged as $x = 1 + \frac{1}{x}$, so we could find successive approximations, x_n, to a root by using the formula

$$x_{n+1} = 1 + \frac{1}{x_n}.$$

If we take $x_1 = 1$ as our initial approximation, we obtain the following:

$$x_1 = 1$$

$$x_2 = 1 + \frac{1}{x_1} = 1 + \frac{1}{1} = \frac{2}{1}$$

$$x_3 = 1 + \frac{1}{x_2} = 1 + \cfrac{1}{1 + \cfrac{1}{1}} = \frac{3}{2}$$

$$x_4 = 1 + \frac{1}{x_3} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{5}{3}$$

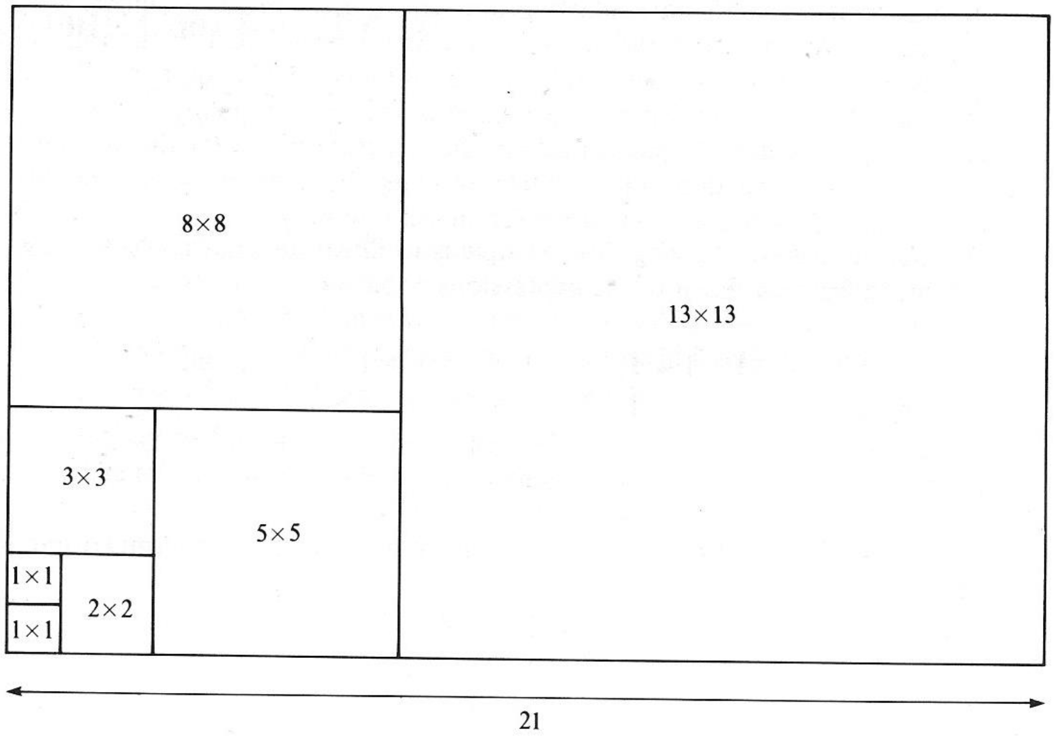
$$x_5 = 1 + \frac{1}{x_4} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}} = \frac{8}{5}, \quad \text{etc.}$$

It is interesting to see the Fibonacci numbers appearing as numerators and denominators of each x_n, and we might make the conjecture that $x_n = \frac{u_{n+1}}{u_n}$, for all positive integers n. This is certainly true when $n = 1$ and, if we assume that $x_k = \frac{u_{k+1}}{u_k}$, then

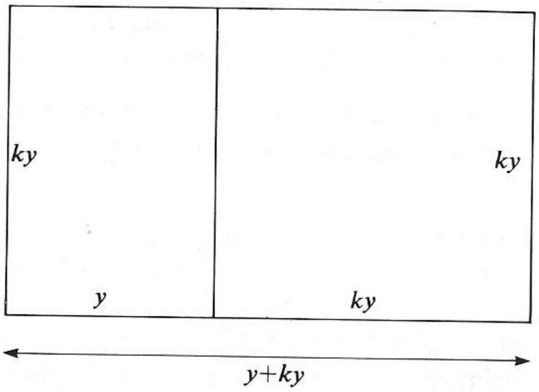
$$x_{k+1} = 1 + \frac{1}{x_k} = 1 + \cfrac{1}{\cfrac{u_{k+1}}{u_k}} = \frac{u_{k+1} + u_k}{u_{k+1}} = \frac{u_{k+2}}{u_{k+1}}.$$

So mathematical induction confirms that it is true that $x_n = \frac{u_{n+1}}{u_n}$ for all $n \geq 1$.

The question remains as to whether or not the sequence $\{x_n\}$ produced by our iterative process converges. This question is the same as asking whether the sequence $\left\{\frac{u_{n+1}}{u_n}\right\}$ of ratios of successive Fibonacci numbers converges, and this problem turns out to have a nice geometric interpretation. Imagine squares with edge-lengths 1, 1, 2, 3, 5, 8, 13, ... These can be joined, in order, to form a sequence of rectangles where, at each stage, the new rectangle is formed by adjoining the next square to the longer edge of the existing rectangle. This process is illustrated by the figure. Now the shape of each rectangle, as determined by the ratio of the longer to the shorter edge, is the ratio of successive Fibonacci numbers. So the question becomes: Does this sequence of rectangles have a limiting shape?



The answer, as we shall see from the work of this unit, is yes. If, for the moment, we assume that the sequence has a limit k, say, then it is not too difficult to see what k must be. For sufficiently large rectangles the ratio of the lengths of the edges is very close to k, so we could take these lengths to be approximately ky and y. To obtain the next rectangle we add on a square of edge-length ky:



The ratio of the lengths of the edges of this rectangle is also approximately k, and so

$$\frac{y+ky}{ky} \simeq k \quad \text{or} \quad k^2 - k - 1 \simeq 0.$$

Hence, if our sequence tends to a limit, it ought to be a root of the original quadratic equation $x^2 - x - 1 = 0$. The positive root is $k = \dfrac{1+\sqrt{5}}{2}$, a number which is known as the *golden ratio*. It has the property that, given any rectangle with edge-lengths in this ratio, then adding a square to the longer edge produces another rectangle with edge-lengths in this same ratio.

The golden ratio first arose from the problem of dividing a line segment AB at a point C such that $\dfrac{AB}{AC} = \dfrac{AC}{CB}$, this common ratio turning out to be $\dfrac{1+\sqrt{5}}{2}$. Like another well known irrational number, π, the golden ratio continually crops up in mathematics, and is particularly prominent in geometrical problems concerning regular plane and solid figures. As one example, it is the ratio of the radius of a circle to the edge-lengths of an inscribed regular decagon. There is little doubt that the golden ratio was used consciously by many Greek architects and sculptors, particularly in the structure of the Parthenon. The Greek theatre at Epidarros has 21 tiers of seats above the gangway and 34 below, 21 and 34 being consecutive Fibonacci numbers.

Our main purpose in giving this example is to illustrate what is meant by a continued fraction. Each of the expressions

$$1, \quad 1+\cfrac{1}{1}, \quad 1+\cfrac{1}{1+\cfrac{1}{1}}, \quad 1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}, \quad \text{etc.}$$

is called a *finite* continued fraction. Their limit is an *infinite* continued fraction, and is written as

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}$$

This is the simplest and most well-known example of a continued fraction. In the more general infinite continued fraction

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}}}$$

the a_i are positive integers, with the exception of a_0 which can be any integer.

The theory of continued fractions is extensive and their area of applicability very wide, so in this unit we can hope only to give you something of the flavour of them.

Section 7.1 is concerned with finite continued fractions and here we do much of the groundwork for subsequent development of properties of infinite continued fractions. Turning to infinite continued fractions in Section 7.2, the main problem confronting us is the question of convergence. We shall discover that every infinite continued fraction converges to an irrational number, and in Section 7.3 we settle the converse problem by showing that every irrational number can be expressed, in a unique way, as an infinite continued fraction. In Section 7.4, we break the irrational numbers down further by classifying, in terms of their continued fractions, those numbers which arise as irrational roots of quadratic equations.

We are all in the habit of writing down, and even manipulating, expressions such as π, $\log_e 3$, $\frac{1+\sqrt{5}}{2}$, etc., which represent irrational numbers. But when it comes to practical calculations we must deal with rational numbers. (Even today's computers are limited in how many decimal places of π they can handle.) So the question of finding good rational approximations to irrational numbers such as $\log_e 3$ is important. In Section 7.5, the final section of the unit, we see how the continued fraction of an irrational number provides us with 'best possible' rational approximations.

The unit is based on Sections 13.3 and 13.4 of **B**.

7.1 Finite Continued Fractions

READ B Section 13.3, page 299 as far as page 304, line 15.

NOTES (i) *Page 300, line 11*

Because the numerators are not ones, Bombelli's example is not a continued fraction in the sense of Definition 13-1. It turns out that our insistence that the numerators must be ones does not impose any restriction, since every number has a continued fraction in this form. In Section 7.4 we shall find the 'correct' continued fraction for $\sqrt{13}$.

It may be far from obvious to you why Bombelli's example does give $\sqrt{13}$. The following non-rigorous argument, which ignores all the real problems of convergence, might at least convince you that the result is correct. If we *assume* that

$$x = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}$$

then adding 3 to both sides gives

$$x + 3 = 6 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}$$

But this is the denominator of the first 4 in the expression for x, so substituting we get

$$x = 3 + \frac{4}{x + 3}$$

which simplifies to $x^2 = 13$. Finally, since everything in sight is positive, we can discard the negative root and conclude $x = \sqrt{13}$.

(ii) *Page 301, line 3*

Any rational number, positive or negative, can be written with the denominator positive. Writing the number in this form before applying the Euclidean algorithm guarantees that only a_0 amongst the a_i can possibly be negative.

(iii) *Page 302, line 7*

The complete Euclidean algorithm appropriate to finding the continued fraction for 19/51 should be

$$19 = \underline{0} \cdot 51 + 19$$

$$51 = \underline{2} \cdot 19 + 13$$

$$19 = \underline{1} \cdot 13 + 6$$

$$13 = \underline{2} \cdot 6 + 1$$

$$6 = \underline{6} \cdot 1 + 0.$$

Notice that, like **B**, we have written the products on the right-hand side in our customary way for the Euclidean algorithm, but this reverses the order in which the products appear in the proof of Theorem 13-5. The underlined numbers are the a_i of Theorem 13-5, and these are the partial denominators of the continued fraction. Although **B** restricts the term 'partial denominator' to $a_1, a_2, \ldots$, we occasionally use it loosely to include a_0. So

$$\frac{19}{51} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}} \quad \blacktriangle$$

SAQ 1 **B** page 312, Problems 13.3, number 1.

SAQ 2 **B** page 312, Problems 13.3, number 2.

SAQ 3 **B** page 312, Problems 13.3, number 4.

SOLUTION TO SAQ 1 Using the notation of Note (iii)

(a)
$$\begin{aligned} -19 &= -\underline{1}\cdot 51 + 32 \\ 51 &= \underline{1}\cdot 32 + 19 \\ 32 &= \underline{1}\cdot 19 + 13 \\ 19 &= \underline{1}\cdot 13 + 6 \\ 13 &= \underline{2}\cdot 6 + 1 \\ 6 &= \underline{6}\cdot 1 + 0 \end{aligned}$$

So $-\frac{19}{51} = [-1; 1, 1, 1, 2, 6]$.

(b)
$$\begin{aligned} 187 &= \underline{3}\cdot 57 + 16 \\ 57 &= \underline{3}\cdot 16 + 9 \\ 16 &= \underline{1}\cdot 9 + 7 \\ 9 &= \underline{1}\cdot 7 + 2 \\ 7 &= \underline{3}\cdot 2 + 1 \\ 2 &= \underline{2}\cdot 1 + 0 \end{aligned}$$

So $\frac{187}{57} = [3; 3, 1, 1, 3, 2]$.

(c)
$$\begin{aligned} 71 &= \underline{1}\cdot 55 + 16 \\ 55 &= \underline{3}\cdot 16 + 7 \\ 16 &= \underline{2}\cdot 7 + 2 \\ 7 &= \underline{3}\cdot 2 + 1 \\ 2 &= \underline{2}\cdot 1 + 0 \end{aligned}$$

So $\frac{71}{51} = [1; 3, 2, 3, 2]$.

(d)
$$\begin{aligned} 118 &= \underline{0}\cdot 303 + 118 \\ 303 &= \underline{2}\cdot 118 + 67 \\ 118 &= \underline{1}\cdot 67 + 51 \\ 67 &= \underline{1}\cdot 51 + 16 \\ 51 &= \underline{3}\cdot 16 + 3 \\ 16 &= \underline{5}\cdot 3 + 1 \\ 3 &= \underline{3}\cdot 1 + 0 \end{aligned}$$

So $\frac{118}{303} = [0; 2, 1, 1, 3, 5, 3]$. ■

SOLUTION TO SAQ 2 (a)
$$[-2; 2, 4, 6, 8] = -2 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{6 + \cfrac{1}{8}}}} = -2 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{8}{49}}}$$

$$= -2 + \cfrac{1}{2 + \cfrac{49}{204}} = -2 + \frac{204}{457} = -\frac{710}{457}.$$

(b) $[4; 2, 1, 3, 1, 2, 4] = \frac{741}{170}$.

(c) $[0; 1, 2, 3, 4, 3, 2, 1] = \frac{321}{460}$.

COMMENT You will no doubt be relieved to hear that we shall shortly discover a far simpler method of calculating these continued fractions. ■

SOLUTION TO SAQ 3

(a) $[0; 3, 1, 2, 3] = [0; 3, 1, 2, 2, 1]$, since $3 = 2 + \frac{1}{1}$.

(b) $[-1; 2, 1, 6, 1] = [-1; 2, 1, 7]$, since $6 + \frac{1}{1} = 7$.

(c) $[2; 3, 1, 2, 1, 1, 1] = [2; 3, 1, 2, 1, 2]$, since $1 + \frac{1}{1} = 2$. ■

In SAQ 2 we computed continued fractions in what looks like the only logical way, starting with the final partial denominator and systematically working our way upward, calculating the various fractions along the way. In the next reading passage we learn an alternative method which starts at the other end, successively calculating the continued fractions in the sequence

$$[a_0], [a_0; a_1], [a_0; a_1, a_2], \ldots, [a_0; a_1, a_2, \ldots, a_n].$$

As the continued fraction we want is the last term of this sequence, this may look like a lot of unnecessary work. It turns out, however, that each member of the sequence (from the third onwards) is easily calculated from the previous two without even involving fractions or common denominators.

READ B from page 304, line -10 to page 307, line 4.

NOTES (i) *Page 304, last line*

Although the formula given here is quite clearly valid, it must be noted that, except when $a_{k+1} = 1$, $a_k + \frac{1}{a_{k+1}}$ is not an integer and consequently $\left[a_0; a_1, a_2, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right]$ is not a *simple* continued fraction. This result is therefore set in the context of the more general continued fraction, where we adopt the same notation. The result is used later in the proof of the important Theorem 13-6.

(ii) *Page 306, line 12*

There is a slight flaw in the inductive proof of Theorem 13-6. In Note (i) we observed that $\left[a_0; a_1, a_2, \ldots, a_m + \frac{1}{a_{m+1}}\right]$ is not in general a *simple* continued fraction, so the replacement of a_m by $a_m + \frac{1}{a_{m+1}}$ is not justified by the inductive hypothesis.

Fortunately, this flaw is easily remedied since the result of Theorem 13-6 happens to be true for any continued fraction, simple or not. All we need do is omit the word 'simple' from the statement of the theorem and the words 'the integers' from line 8. The formulae for C_0, C_1 and C_2 (on page 305) which launch the induction, remain valid, and now the critical stage of the inductive step, replacing a_m by $a_m + \frac{1}{a_{m+1}}$, creates no problems. So we have a valid proof of Theorem 13-6 for the more general continued fractions. As an immediate corollary, it holds for simple continued fractions, which are our immediate interest. ▲

Notice that, for simple continued fractions, the denominator q_k of the convergent C_k is positive for $k \geq 0$. Certainly $q_0 = 1$ and $q_1 = a_1 \geq 1$ are both positive, and the inductive step is provided by the formula $q_k = a_k q_{k-1} + q_{k-2}$ for $k \geq 2$.

The formulae in the middle of page 305 are crucial. In what follows we shall use them many times, primarily for calculating convergents of a continued fraction but also for theoretical considerations. The SAQs in the unit will provide you with plenty of opportunities to practise using them.

In the following example we suggest a tabular method for calculating the successive numerators and denominators. This method may help you avoid arithmetic slips and might assist you in remembering these important formulae. After SAQ 4, which follows, we shall not use tables again, but you might like to persist with this method.

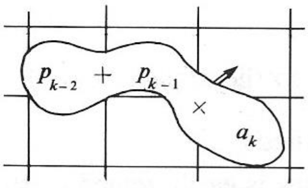
EXAMPLE 1 Determine the rational number represented by

$$[4; 2, 1, 3, 1, 2, 4].$$

In the tabular method we set out four rows labelled k, p_k, a_k and q_k. The a_k are the given partial denominators and so the entries for this row, and the k row, can be displayed immediately. The p_k and q_k rows are started by entering the first two values for each, using the formulae $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ and $q_1 = a_1$. For our particular example these are $p_0 = 4$, $p_1 = 9$, $q_0 = 1$ and $q_1 = 2$, and the initial table is

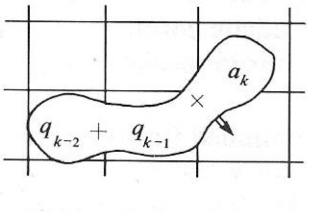
k	0	1	2	3	4	5	6
p_k	4	9					
a_k	4	2	1	3	1	2	4
q_k	1	2					

To complete the table we move along the a_k row filling in the entries above and below each a_k. For the entry above a_k (i.e. p_k) we multiply a_k by the entry diagonally above to the left, and add to this product the entry to the left of the latter. So, for example, $p_2 = (1 \cdot 9) + 4 = 13$, and then $p_3 = (3 \cdot 13) + 9 = 48$.



$$p_k = a_k p_{k-1} + p_{k-2}$$

The same procedure applies for the q_k. We multiply a_k by the entry diagonally below to the left and add on the entry to the left of that. So $q_2 = (1 \cdot 2) + 1 = 3$, and so on.



$$q_k = a_k q_{k-1} + q_{k-2}$$

The complete table is

k	0	1	2	3	4	5	6
p_k	4	9	13	48	61	170	741
a_k	4	2	1	3	1	2	4
q_k	1	2	3	11	14	39	170

and the successive convergents $\frac{p_k}{q_k}$ are $\frac{4}{1}, \frac{9}{2}, \frac{13}{3}, \frac{48}{11}, \frac{61}{14}, \frac{170}{39}$ and $\frac{741}{170}$, the last being the value of the continued fraction.

In our solution to SAQ 4 we have used the tabular method for parts (a) and (b). For part (c) we have used formula $(*)$ of Theorem 13-6, calculating the successive numerators and denominators (and therefore the convergents) simultaneously.

SAQ 4 **B** page 312, Problems 13.3, number 5.

SOLUTION TO SAQ 4 (a)

k	0	1	2	3	4	5
p_k	1	3	10	33	76	109
a_k	1	2	3	3	2	1
q_k	1	2	7	23	53	76

The convergents are $\frac{1}{1}, \frac{3}{2}, \frac{10}{7}, \frac{33}{23}, \frac{76}{53}$ and $\frac{109}{76}$.

(b)

k	0	1	2	3	4	5
p_k	-3	-2	-5	-7	-12	-43
a_k	-3	1	1	1	1	3
q_k	1	1	2	3	5	18

The convergents are $\frac{-3}{1}, \frac{-2}{1}, \frac{-5}{2}, \frac{-7}{3}, \frac{-12}{5}$ and $\frac{-43}{18}$.

(c) Using $(*)$, the sequence of convergents of $[0; 2, 4, 1, 8, 2]$ is

$$\frac{0}{1}, \frac{1}{2}, \frac{(4\cdot1)+0}{(4\cdot2)+1} = \frac{4}{9}, \quad \frac{(1\cdot4)+1}{(1\cdot9)+2} = \frac{5}{11}, \quad \frac{(8\cdot5)+4}{(8\cdot11)+9} = \frac{44}{97},$$

$$\frac{(2\cdot44)+5}{(2\cdot97)+11} = \frac{93}{205}. \quad ■$$

The next reading passage shows how continued fractions can be used to give a good method of solving linear Diophantine equations.

READ B from page 307, line 7 to page 310, line 15.

SAQ 5 **B** page 313, Problems 13.3, number 11.

SOLUTION TO SAQ 5

(a) The continued fraction for $\frac{51}{19}$ is $[2; 1, 2, 6]$ and the convergents are $\frac{2}{1}$, $\frac{3}{1}$, $\frac{8}{3}$ and $\frac{51}{19}$. So by Theorem 13-7, $51 \cdot 3 - 19 \cdot 8 = (-1)^{3-1} = 1$ giving one solution $x_0 = -8$, $y_0 = 3$. The general solution is

$$\{x = -8 + 51t,\ y = 3 - 19t\colon t \in \mathbb{Z}\}.$$

COMMENT We could have started by finding the continued fraction for $\frac{19}{51}$, which would have been slightly longer since it has an extra partial denominator. Whichever method you use, make sure that you do not end up with the x and y values the wrong way around!

(b) The continued fraction for $\frac{364}{227}$ is $[1; 1, 1, 1, 1, 10, 1, 3]$ and the convergents are $\frac{1}{1}$, $\frac{2}{1}$, $\frac{3}{2}$, $\frac{5}{3}$, $\frac{8}{5}$, $\frac{85}{53}$, $\frac{93}{58}$ and $\frac{364}{227}$. So $364 \cdot 58 - 227 \cdot 93 = 1$, giving one solution $x_0 = 58$, $y_0 = -93$. The general solution is

$$\{x = 58 + 227t,\ y = -93 - 364t\colon t \in \mathbb{Z}\}.$$

(c) We first consider the equation $18x + 5y = 1$. The continued fraction for $\frac{18}{5}$ is $[3; 1, 1, 2]$ and the convergents are $\frac{3}{1}$, $\frac{4}{1}$, $\frac{7}{2}$ and $\frac{18}{5}$. Therefore $18 \cdot 2 - 5 \cdot 7 = 1$, from which we obtain $18 \cdot (2 \cdot 24) - 5 \cdot (7 \cdot 24) = 24$. This gives a particular solution $x_0 = 48$, $y_0 = -168$ of our original equation, and consequently the general solution is

$$\{x = 48 + 5t,\ y = -168 - 18t\colon t \in \mathbb{Z}\}.$$

(d) The continued fraction for $\frac{158}{57}$ is $[2; 1, 3, 2, 1, 1, 2]$ and the convergents are $\frac{2}{1}$, $\frac{3}{1}$, $\frac{11}{4}$, $\frac{25}{9}$, $\frac{36}{13}$, $\frac{61}{22}$ and $\frac{158}{57}$. Therefore $158 \cdot 22 - 57 \cdot 61 = -1$. That is, $158 \cdot (-22) - 57 \cdot (-61) = 1$ giving $x_0 = -22$, $y_0 = -61$ as one solution. The general solution is

$$\{x = -22 + 57t,\ y = -61 + 158t\colon t \in \mathbb{Z}\}. \quad ■$$

In the final reading passage of this section, we prove a result concerning the behaviour of the convergents of a continued fraction. This will play an important part in settling the question of convergence for infinite continued fractions, which we shall be turning to in the next section.

READ B from page 310, line −12 to the end of Section 13.3.

NOTE *Page 310, line −9*

The proof of the Lemma is not by induction at all. Having catered for the special case $q_0 \leq q_1$, for $k \geq 2$ we have

$$q_k = a_k q_{k-1} + q_{k-2} > a_k q_{k-1} \qquad (\text{since } q_{k-2} > 0)$$

and

$$a_k q_{k-1} \geq q_{k-1} \qquad (\text{since } a_k \geq 1).$$

Therefore $q_k > q_{k-1}$, for all $k \geq 2$. ▲

SAQ 6 Calculate the convergents of the following continued fractions and in each case verify Theorem 13-8:

(a) $[1; 2, 2, 2, 2, 2, 2,]$; (b) $[2; 2, 4, 2, 4, 2, 4]$.

SOLUTION TO SAQ 6

(a) The convergents are $C_0 = 1$, $C_1 = \frac{3}{2}$, $C_2 = \frac{7}{5}$, $C_3 = \frac{17}{12}$, $C_4 = \frac{41}{29}$, $C_5 = \frac{99}{70}$ and $C_6 = \frac{239}{169}$. Theorem 13-8 says that $C_0 < C_2 < C_4 < C_6 < C_5 < C_3 < C_1$ which we can confirm by evaluating the convergents to 4 decimal places:

$$1 < 1.4 < 1.4138 < 1.4142 < 1.4143 < 1.4167 < 1.5.$$

(b) The convergents are $C_0 = 2$, $C_1 = \frac{5}{2}$, $C_2 = \frac{22}{9}$, $C_3 = \frac{49}{20}$, $C_4 = \frac{218}{89}$, $C_5 = \frac{485}{198}$ and $C_6 = \frac{2158}{881}$. Theorem 13-8 says that

$$C_0 < C_2 < C_4 < C_6 < C_5 < C_3 < C_1.$$

In confirming this, to distinguish between C_5 and C_6 we have to approximate these rational numbers to 6 decimal places:

$$2 < 2.444444 < 2.449438 < 2.449489 < 2.449495 < 2.45 < 2.5.$$

COMMENT A rather more elegant way of verifying that $\dfrac{c}{d} < \dfrac{a}{b}$ is to calculate $ad - bc$ and show that it is positive. For the verification $C_6 < C_5$ we find $485 \cdot 881 - 2158 \cdot 198 = 1$, as we expect from Theorem 13-7. ■

7.2 Infinite Continued Fractions

We now consider infinite continued fractions, for which we have a natural extension of the notation of the previous section, using $[a_0; a_1, a_2, a_3, \ldots]$ for the continued fraction with partial denominators (including a_0) $a_0, a_1, a_2, a_3, \ldots$. We shall not use the adjective *simple* in connection with infinite continued fractions for it is to be understood that in any infinite continued fraction each of the a_i is a positive integer, with the exception of a_0 which may be negative. Note, however, that the coming work necessarily involves finite continued fractions which are not simple.

The first task confronting us concerns the question of convergence. Whereas the calculation of a finite continued fraction requires only the normal rules of arithmetic, the infinite continued fraction is an infinite process and as such requires a completely different approach. There is a strong resemblance to infinite series. For the latter, we define the infinite sum $\sum_{r=1}^{\infty} a_r$ to be the limit of the sequence $\left\{ \sum_{r=1}^{N} a_r \right\}$ of partial sums, provided this limit exists. For infinite continued fractions, the convergents play the rôle of the partial sums and so, by analogy, we define the value of the infinite continued fraction to be the limit (if it exists) of the sequence $\{C_N\}$ of its convergents.

READ B Section 13.4, page 313 as far as the foot of page 315.

NOTES

(i) *Page 314, line 12*
For the moment **B** shows only the existence of the limit, leaving the proof that it is irrational until later.

(ii) *Page 314, line −8*
By the Lemma, **B** page 310, the $q_k (k > 1)$ are a strictly increasing sequence of integers, and thus increase without bound.

(iii) *Page 315, line −7*
B also uses the notation $[\overline{a_0; a_1, a_2, \ldots, a_n}]$ for the infinite continued fraction $[a_0; a_1, \ldots, a_n, a_0, a_1, \ldots, a_n, a_0, \ldots]$. (Notice that for this it is necessary that the integer a_0 be positive). Such periodic continued fractions are called *purely periodic*. ▲

The values of periodic fractions are readily calculated, as the following examples illustrate.

EXAMPLE 2 We shall find the value of the purely periodic continued fraction $[\overline{1;3,2}]$.

In practice, we would proceed as follows. Letting $x = [\overline{1;3,2}]$ we observe that $x = [\overline{1;3,2}] = [1;3,2,\overline{1,3,2}]$, so that

$$x = 1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{x}}}$$

This means that we can express x as the finite (though not simple) continued fraction $x = [1;3,2,x]$. Now the convergents to this are $1, \frac{4}{3}, \frac{9}{7}$ and $\frac{9x+4}{7x+3}$, and as the final convergent is equal to x itself, we have

$$x = \frac{9x+4}{7x+3}, \quad \text{or} \quad 7x^2 - 6x - 4 = 0.$$

The positive root (which is clearly the one we want) of this quadratic is $x = \frac{3+\sqrt{37}}{7}$.

The substitution for x in the first step of the above argument takes some liberties with properties of limits. To give the same argument correctly we would, instead, observe that

$$C_n = 1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{C_{n-3}}}} \qquad (\text{for } n \geq 3)$$

which gives $C_n = \frac{9C_{n-3}+4}{7C_{n-3}+3}$. Now from the definition of $x = [\overline{1;3,2}]$,

$$x = \lim_{n\to\infty} C_n = \lim_{n\to\infty} C_{n-3},$$

so taking limits of both sides of the above equation gives $x = \frac{9x+4}{7x+3}$, as before.

The underlying ideas of this example will work for any purely periodic continued fraction. For if $x = [\overline{a_0; a_1, a_2, \ldots, a_n}]$ $(a_0 \geq 1)$, then $x = [a_0; a_1, a_2, \ldots, a_n, x]$. With the usual notation, the final three convergents in this finite continued fraction are $\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$ and $\frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$. As the latter is equal to x, we arrive at the quadratic $q_n x^2 + (q_{n-1} - p_n)x - p_{n-1} = 0$ whose positive root is the value of the continued fraction.

EXAMPLE 3 Consider $y = [2; 5, \overline{1,3,2}] = 2 + \cfrac{1}{5 + \cfrac{1}{x}}$, where $x = \frac{3+\sqrt{37}}{7}$ as discovered in Example 2. The convergents to $y = [2;5,x]$ are $2, \frac{11}{5}, \frac{11x+2}{5x+1}$, and so

$$y = \frac{11x+2}{5x+1} = \frac{11\left(\frac{3+\sqrt{37}}{7}\right)+2}{5\left(\frac{3+\sqrt{37}}{7}\right)+1} = \frac{47+11\sqrt{37}}{22+5\sqrt{37}}.$$

Rationalizing, by multiplying top and bottom by $22 - 5\sqrt{37}$, this simplifies to $y = \dfrac{143 - \sqrt{37}}{63}$.

This example illustrates how to calculate any periodic continued fraction $y = [a_0; a_1, a_2, \ldots, a_m, \overline{b_1, b_2, \ldots, b_n}]$. We first calculate $x = [\overline{b_1; b_2, b_3, \ldots, b_n}]$ by the method of Example 2 and then obtain $y = [a_0; a_1, a_2, \ldots, a_m, x]$ by the method of Example 3.

If you glance ahead to page 317 of **B**, you will find another example of this type, Example 13-4.

SAQ 7 Evaluate the continued fractions:

(a) $[\overline{1;2}]$, (b) $[1;\overline{1,2}]$, (c) $[2;\overline{1,1,1,4}]$, (d) $[-2;1,2,\overline{3,4}]$.

SOLUTION TO SAQ 7 (a) Let $x = [\overline{1;2}] = [1;2,\overline{1,2}] = 1 + \cfrac{1}{2 + \cfrac{1}{x}} = \dfrac{3x+1}{2x+1}$. Therefore

$2x^2 - 2x - 1 = 0$, which has positive root $x = \dfrac{1+\sqrt{3}}{2}$.

(b) Let $y = [1;\overline{1,2}] = [1;x] = 1 + \dfrac{1}{x}$, where $x = \dfrac{1+\sqrt{3}}{2}$ from (a). Therefore

$$y = 1 + \frac{2}{1+\sqrt{3}} = \frac{3+\sqrt{3}}{1+\sqrt{3}} \cdot \frac{1-\sqrt{3}}{1-\sqrt{3}} = \sqrt{3}.$$

(c) Let $x = [\overline{1;1,1,4}] = [1;1,1,4,x]$. The convergents are $1, \dfrac{2}{1}, \dfrac{3}{2}, \dfrac{14}{9}$ and $\dfrac{14x+3}{9x+2}$. Therefore $x = \dfrac{14x+3}{9x+2}$, giving $3x^2 - 4x - 1 = 0$, whose positive root is $x = \dfrac{2+\sqrt{7}}{3}$. Now,

$$[2;\overline{1,1,1,4}] = [2;x] = 2 + \frac{1}{x} = 2 + \frac{3}{2+\sqrt{7}} = \sqrt{7}.$$

(d) Let $x = [\overline{3;4}] = [3;4,x] = 3 + \cfrac{1}{4 + \cfrac{1}{x}}$. So $x = \dfrac{13x+3}{4x+1}$, giving

$4x^2 - 12x - 3 = 0$, or $x = \dfrac{3+2\sqrt{3}}{2}$.

Now,

$$[-2;1,2,\overline{3,4}] = [-2;1,2,x] = \frac{-4x-1}{3x+1} = \frac{-14-8\sqrt{3}}{11+6\sqrt{3}} = \frac{-10-4\sqrt{3}}{13}. \quad \blacksquare$$

In the final reading passage of this section we prove two important results concerning infinite continued fractions. First we confirm that the value of any infinite continued fraction is an irrational number; and second, in anticipation of the converse result, we prove that the continued fraction of an irrational number is unique.

READ B from the top of page 316 as far as page 317, line −13.

NOTE *Page 316, bottom*

The observation made here can be extended in an obvious way:

$$[a_0;a_1,a_2,\ldots] = a_0 + \cfrac{1}{[a_1;a_2,a_3,\ldots]}$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{[a_2;a_3,a_4,\ldots]}}$$

and these results provide a rigorous basis for the intuitive arguments used in our Examples 2 and 3. **B** is quite right to give justification, for when dealing with infinite sums, nothing is obvious! ▲

SAQ 8 **B** page 327, Problems 13.4, number 2.

SOLUTION TO SAQ 8 Consider $[0;\, a_0,\, a_1,\, a_2,\ldots]$. (Notice that $x > 1$ ensures that $a_0 \geq 1$ and so this is an infinite continued fraction.) By the result at the foot of page 316,

$$[0;\, a_0,\, a_1,\, a_2,\ldots] = 0 + \cfrac{1}{[a_0;a_1,a_2,\ldots]} = \frac{1}{x}.$$

Using this result with $x = [1;\bar{1}]$ we see that $[0;\bar{1}] = \dfrac{1}{x}$. However, we have already seen on page 315 that $[1;\bar{1}] = \dfrac{1+\sqrt{5}}{2}$, so

$$[0;\bar{1}] = \frac{2}{1+\sqrt{5}} = \frac{\sqrt{5}-1}{2}. \quad ■$$

7.3 The Continued Fraction Algorithm

We have now seen that every infinite continued fraction represents an irrational number. We are left with the question of whether *every* irrational number has an infinite continued fraction. In this section we show that the answer is yes, and Theorem 13-10 confirms that the infinite continued fraction of an irrational number is unique.

If, for the moment, we assume that the irrational number x_0 has an infinite continued fraction, say $x_0 = [a_0;\, a_1,\, a_2,\, a_3,\ldots,]$, then the proof of Theorem 13-10 tells us exactly what the a_i must be.

We know already that $a_0 = [x_0]$, the integer part of x_0, and furthermore

$$x_0 = a_0 + \frac{1}{[a_1;a_2,a_3,\ldots]} = [x_0] + \frac{1}{[a_1;a_2,a_3,\ldots]}.$$

But this gives $\dfrac{1}{x_0 - [x_0]} = [a_1;a_2,a_3,\ldots]$.

Now if we put $x_1 = \dfrac{1}{x_0 - [x_0]}$, which, like x_0, is irrational, then

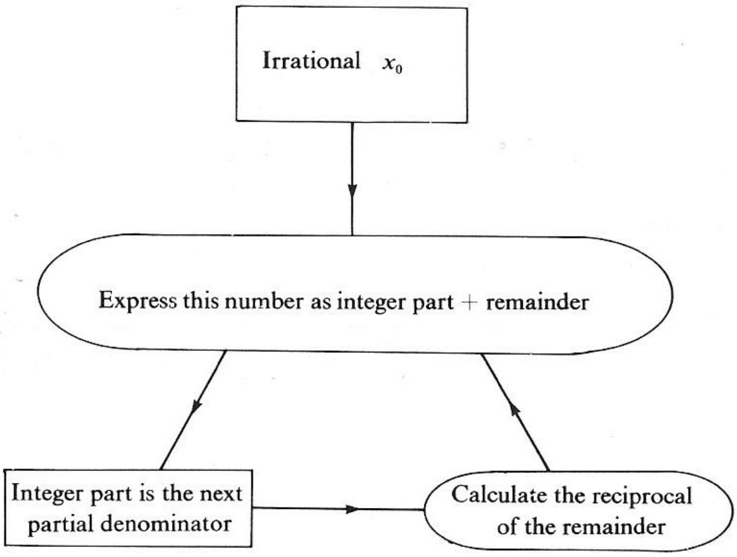
$x_1 = [a_1;a_2,a_3,\ldots]$. As before, $a_1 = [x_1]$ and

$$x_1 = a_1 + \frac{1}{[a_2;a_3,\ldots]} = [x_1] + \frac{1}{[a_2;a_3,\ldots]}$$

And so we can continue, $x_2 = \dfrac{1}{x_1 - [x_1]}$ (an irrational), which leads to

$a_2 = [x_2]$, and so on.

In fact we have a procedure (known as the Continued Fraction Algorithm) for computing successive partial denominators for the continued fraction of x_0, which is summed up in the following flow chart.


Irrational x_0
Express this number as integer part + remainder
Integer part is the next partial denominator
Calculate the reciprocal of the remainder

Of course, it still remains to show that the infinite continued fraction determined by this process converges to the original irrational number x_0. The proof of this is contained in the next reading passage from **B**, but before that let us assume the result and illustrate the algorithm in action.

EXAMPLE 4 In Section 7.1, we saw Bombelli's continued fraction for $\sqrt{13}$. We shall now find the 'correct' one.

Suppose $\sqrt{13}$ has continued fraction $[a_0; a_1, a_2, a_3, \ldots]$. We follow the above algorithm.

$$x_0 = \sqrt{13} = 3.6055\ldots,$$

so $a_0 = [x_0] = 3$ and $x_0 - [x_0] = \sqrt{13} - 3$.

$$x_1 = \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{13} - 3} = \frac{1}{\sqrt{13} - 3} \cdot \frac{\sqrt{13} + 3}{\sqrt{13} + 3} = \frac{\sqrt{13} + 3}{4}$$

$$= \frac{6.6055\ldots}{4} = 1 + \left(\frac{\sqrt{13} - 1}{4}\right),$$

so $a_1 = 1$ and $x_1 - [x_1] = \dfrac{\sqrt{13} - 1}{4}$.

$$x_2 = \frac{1}{x_1 - [x_1]} = \frac{4}{\sqrt{13} - 1} = \frac{\sqrt{13} + 1}{3} = \frac{4.6055\ldots}{3} = 1 + \left(\frac{\sqrt{13} - 2}{3}\right),$$

so $a_2 = 1$ and $x_2 - [x_2] = \dfrac{\sqrt{13} - 2}{3}$.

$$x_3 = \frac{1}{x_2 - [x_2]} = \frac{3}{\sqrt{13} - 2} = \frac{\sqrt{13} + 2}{3} = 1 + \left(\frac{\sqrt{13} - 1}{3}\right),$$

so $a_3 = 1$ and $x_3 - [x_3] = \dfrac{\sqrt{13} - 1}{3}$.

$$x_4 = \frac{1}{x_3 - [x_3]} = \frac{3}{\sqrt{13} - 1} = \frac{\sqrt{13} + 1}{4} = 1 + \left(\frac{\sqrt{13} - 3}{4}\right),$$

so $a_4 = 1$ and $x_4 - [x_4] = \dfrac{\sqrt{13} - 3}{4}$.

$$x_5 = \frac{1}{x_4 - [x_4]} = \frac{4}{\sqrt{13}-3} = \sqrt{13}+3 = 6.6055\ldots = 6 + (\sqrt{13}-3),$$

so $a_5 = 6$ and $x_5 - [x_5] = \sqrt{13} - 3$.

But now $x_6 = \dfrac{1}{\sqrt{13}-3} = x_1$, implying that $a_6 = a_1$. Moreover, $x_7 = \dfrac{1}{x_6 - [x_6]}$ $= \dfrac{1}{x_1 - [x_1]} = x_2$ gives $a_7 = a_2$. Clearly, we are in a cycle, and the sequence of partial denominators 1, 1, 1, 1, 6 will recur indefinitely. So, assuming that $\sqrt{13}$ can be expressed as an infinite continued fraction, it must be $[3;\overline{1,1,1,1,6}]$.

READ B from page 318, line 5 to page 323, line 9.

NOTES (i) *Page 319, line 11*

Recall the convention for convergents. C_n is called the nth convergent. However, as C_0 is the zeroth convergent, there are in all, up to and including C_n, $n+1$ convergents.

On line 14, C'_{n+1} is the last convergent of the finite continued fraction on the previous line, and as such is the value of the fraction itself.

(ii) *Page 319, line −10*

Once again, the argument here requires our stronger form of the fraction itself. Theorem 13-6, where the contined fraction is not required to be simple. ▲

SAQ 9 **B** page 327, Problems 13.4, number 4 parts (a), (d) and (e).

SAQ 10 **B** page 327, Problems 13.4, number 5.

SOLUTION TO SAQ 9 (a) $\sqrt{5} = 2.236\ldots$

$$x_0 = \sqrt{5} = 2 + (\sqrt{5}-2), \qquad a_0 = 2$$

$$x_1 = \frac{1}{\sqrt{5}-2} = \sqrt{5}+2 = 4 + (\sqrt{5}-2), \qquad a_1 = 4$$

$x_2 = \dfrac{1}{\sqrt{5}-2} = x_1$, and so we are in a cycle with $4 = a_1 = a_2 = a_3 = \ldots$.

Therefore $\sqrt{5} = [2;\overline{4}]$.

(d) $\sqrt{37} = 6.083\ldots$

$$x_0 = \frac{5+\sqrt{37}}{4} = 2 + \left(\frac{\sqrt{37}-3}{4}\right), \qquad a_0 = 2$$

$$x_1 = \frac{4}{\sqrt{37}-3} = \frac{\sqrt{37}+3}{7} = 1 + \left(\frac{\sqrt{37}-4}{7}\right), \qquad a_1 = 1$$

$$x_2 = \frac{7}{\sqrt{37}-4} = \frac{\sqrt{37}+4}{3} = 3 + \left(\frac{\sqrt{37}-5}{3}\right), \qquad a_2 = 3$$

$x_3 = \dfrac{3}{\sqrt{37}-5} = \dfrac{\sqrt{37}+5}{4} = x_0$, and so we are in a cycle starting with $a_3 = a_0$. Therefore $\dfrac{5+\sqrt{37}}{4} = [\overline{2;1,3}]$.

(e) $\sqrt{30} = 5.477\ldots$

$$x_0 = \frac{11+\sqrt{30}}{13} = 1 + \left(\frac{\sqrt{30}-2}{13}\right), \qquad a_0 = 1$$

$$x_1 = \frac{13}{\sqrt{30}-2} = \frac{\sqrt{30}+2}{2} = 3 + \left(\frac{\sqrt{30}-4}{2}\right), \qquad a_1 = 3$$

$$x_2 = \frac{2}{\sqrt{30}-4} = \frac{\sqrt{30}+4}{7} = 1 + \left(\frac{\sqrt{30}-3}{7}\right), \qquad a_2 = 1$$

$$x_3 = \frac{7}{\sqrt{30}-3} = \frac{\sqrt{30}+3}{3} = 2 + \left(\frac{\sqrt{30}-3}{3}\right), \qquad a_3 = 2$$

$$x_4 = \frac{3}{\sqrt{30}-3} = \frac{\sqrt{30}+3}{7} = 1 + \left(\frac{\sqrt{30}-4}{7}\right), \qquad a_4 = 1$$

$$x_5 = \frac{7}{\sqrt{30}-4} = \frac{\sqrt{30}+4}{2} = 4 + \left(\frac{\sqrt{30}-4}{2}\right), \qquad a_5 = 4$$

$x_6 = \dfrac{2}{\sqrt{30}-4} = x_2$, so we are in a cycle starting with $a_6 = a_2$.

Therefore $\dfrac{11+\sqrt{30}}{13} = [1;3, \overline{1, 2, 1, 4}]$. ■

SOLUTION TO SAQ 10

(a) Using the hint, we see that $\sqrt{n^2+1} = n + \dfrac{1}{n+\sqrt{n^2+1}}$ where, clearly, $0 < \dfrac{1}{n+\sqrt{n^2+1}} < 1$. Therefore

$$x_0 = \sqrt{n^2+1} = n + \left(\frac{1}{n+\sqrt{n^2+1}}\right), \qquad a_0 = n$$

$$x_1 = n + \sqrt{n^2+1} = 2n + (\sqrt{n^2+1} - n) = 2n + \frac{1}{n+\sqrt{n^2+1}}, \qquad a_1 = 2n$$

$x_2 = n + \sqrt{n^2+1} = x_1$, and so we are in a cycle with $2n = a_1 = a_2 = \ldots$.

Hence $\sqrt{n^2+1} = [n;\overline{2n}]$.

$x_0 = \sqrt{n^2+2} = n + (\sqrt{n^2+2} - n)$, where

$$0 < \sqrt{n^2+2} - n = \frac{2}{\sqrt{n^2+2}+n} < 1, \qquad a_0 = n$$

$$x_1 = \frac{1}{\sqrt{n^2+2}-n} = \frac{\sqrt{n^2+2}+n}{2} = n + \left(\frac{\sqrt{n^2+2}-n}{2}\right), \qquad a_1 = n$$

$$x_2 = \frac{2}{\sqrt{n^2+2}-n} = \sqrt{n^2+2} + n = 2n + (\sqrt{n^2+2} - n), \qquad a_2 = 2n$$

$x_3 = \dfrac{1}{\sqrt{n^2+2}-n} = x_1$, so we are in a cycle starting with $a_3 = a_1$.

Hence $\sqrt{n^2+2} = [n;\overline{n, 2n}]$.

$$\sqrt{n^2+2n} = n + (\sqrt{n^2+2n} - n), \text{ where}$$

$$0 < \sqrt{n^2+2n} - n = \frac{2n}{\sqrt{n^2+2n}+n} < 1.$$

$$x_0 = n + (\sqrt{n^2+2n} - n), \qquad a_0 = n$$

$$\begin{aligned} x_1 = \frac{1}{\sqrt{n^2+2n}-n} &= \frac{\sqrt{n^2+2n}+n}{2n} \\ &= 1 + \frac{\sqrt{n^2+2n}-n}{2n} \\ &= 1 + \frac{1}{\sqrt{n^2+2n}+n}, \qquad a_1 = 1 \end{aligned}$$

$$x_2 = \sqrt{n^2+2n} + n = 2n + (\sqrt{n^2+2n} - n), \qquad a_2 = 2n$$

$$x_3 = \frac{1}{\sqrt{n^2+2n}-n} = x_1,$$ so we are in a cycle starting with $a_3 = a_1$. Hence

$$\sqrt{n^2+2n} = [n;\overline{1,2n}\,].$$

(b) $\sqrt{2} = \sqrt{1^2+1} = [1;\overline{2}]$

$\sqrt{3} = \sqrt{1^2+2} = [1;\overline{1,2}\,]$

$\sqrt{15} = \sqrt{3^2+2\cdot 3} = [3;\overline{1,6}\,]$

$\sqrt{37} = \sqrt{6^2+1} = [6;\overline{12}]$ ■

The Corollary on **B** page 320 tells us that, with the usual notation for the convergents of the irrational number x,

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

This can be used to predict how accurately the convergents approximate x, or alternatively to select the appropriate convergent for a desired degree of accuracy. We have seen that the first five convergents of π are $\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}$ and $\frac{103993}{33102}$. From the Corollary, $\left|\pi - \frac{22}{7}\right| < \frac{1}{7\cdot 106} = 0.0013\ldots < 0.005$, so certainly $\frac{22}{7}$ gives π accurately to two decimal places. On the other hand, if we want an approximation to π which is accurate to six decimal places, we have only to observe that $\frac{1}{113\cdot 33102} < 0.0000005$ to see that $\frac{355}{133}$ is such an approximation.

SAQ 11 **B** page 327, Problems 13.4, number 6.

SAQ 12 **B** page 328, Problems 13.4, number 7.

SOLUTION TO SAQ 11 $\sqrt{15} = [3;\overline{1,6}\,]$ has convergents $\frac{3}{1}, \frac{4}{1}, \frac{27}{7}, \frac{31}{8}, \frac{213}{55}, \frac{244}{63}, \frac{1677}{433}, \ldots$. As $\frac{1}{63\cdot 433} = 0.000036\ldots < 0.00005$, the convergent $\frac{244}{63}$ is correct to four decimal places. ■

SOLUTION TO SAQ 12

(a) The convergents are $\frac{2}{1}, \frac{3}{1}, \frac{8}{3}, \frac{11}{4}, \frac{19}{7}, \frac{87}{32}, \frac{106}{39}, \frac{193}{71}, \frac{1264}{465}, \ldots$, and as $\frac{1}{71 \cdot 465} = 0.000030\ldots < 0.00005$, the convergent $\frac{193}{71}$ is correct to four decimal places.

(b) If $e < \frac{a}{b} < \frac{87}{32}$, then

$$0 < \frac{87}{32} - \frac{a}{b} < \frac{87}{32} - e = \left| e - \frac{87}{32} \right| < \frac{1}{32 \cdot 39}$$

$\left(\text{by the Corollary, since } \frac{106}{39} \text{ is the convergent following } \frac{87}{32}\right)$. So

$$0 < \frac{87b - 32a}{32b} < \frac{1}{32 \cdot 39}$$

and as $87b - 32a \geq 1$, we must have $b > 39$. ■

7.4 The Continued Fractions of Quadratic Irrationals

The quadratic irrationals are the numbers of the form $r + s\sqrt{d}$, where r and s are rational, $s \neq 0$ and $d > 0$ is a non-square integer. They are the numbers which arise as irrational roots of quadratic equations with integer coefficients. On page 322, **B** remarks that a number x is a quadratic irrational if and only if the continued fraction of x becomes periodic ultimately. In this section, we shall examine this claim, proving the 'if' part. We begin, however, by considering the simpler case of the continued fractions of $\sqrt{d}$, where d is a non-square integer.

At the bottom of page 334 of **B**, there is a table giving the continued fraction of $\sqrt{d}$ for every non-square integer in the range $1 < d \leq 40$. Concealing the remainder of page 334, examine the given table and then have a go at answering the following.

SAQ 13 What common features are there in the continued fractions given in the table on page 334? Conjecture the general form for the continued fraction of $\sqrt{d}$, where d is a non-square positive integer.

SOLUTION TO SAQ 13

From the evidence presented you might have made some of the following observations.

(i) The continued fraction of $\sqrt{d}$ is periodic, with period starting at a_1.

(ii) The final element in the period is $2a_0$.

(iii) Leaving aside the final term, $2a_0$, the remainder of the period is symmetric (palindromic), reading the same forwards as backwards. In some cases, such as $\sqrt{2}$, $\sqrt{5}$ and $\sqrt{10}$, this symmetric part is non-existent.

Collecting all this together, we might conjecture that the continued fraction of $\sqrt{d}$ takes the form

$$\sqrt{d} = [a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}].$$

COMMENT We can express this conjecture in an equivalent and more succinct form by observing that if it is true, then $[\sqrt{d}] = a_0$ so that

$$\begin{aligned} [\sqrt{d}] + \sqrt{d} &= [2a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}] \\ &= [\overline{2a_0; a_1, a_2, a_3, \ldots, a_3, a_2, a_1}] \end{aligned}$$

which is purely periodic. ■

By the end of this section we shall have gone some way towards proving the conjecture in SAQ 13. As a start in that direction, we investigate the relationship between a purely periodic continued fraction and the fraction obtained by reversing the order of the elements in its cycle.

EXAMPLE 5 Let $\alpha = [\overline{2;1,4,1}]$ and $\beta = [\overline{1;4,1,2}]$ (obtained by reversing the period of α). How, if at all, are α and β related?

Writing $\alpha = [\overline{2;1,4,1}] = [2;1,4,1,\alpha]$, the convergents of the latter are $\frac{2}{1}, \frac{3}{1}, \frac{14}{5}, \frac{17}{6}$ and $\frac{17\alpha+14}{6\alpha+5} = \alpha$, so that α is the positive root of

$$6\alpha^2 - 12\alpha - 14 = 0. \tag{1}$$

Similarly, $\beta = [\overline{1;4,1,2}]$ has convergents $1, \frac{5}{4}, \frac{6}{5}, \frac{17}{14}$ and $\frac{17\beta+6}{14\beta+5} = \beta$, giving

$$14\beta^2 - 12\beta - 6 = 0 \tag{2}$$

of which β is the positive root.

One cannot help noticing the similarity between the coefficients of the quadratics (1) and (2). Indeed, if we substitute $\alpha = \frac{-1}{\beta}$ in (1) we get (2). This means that α and $\frac{-1}{\beta}$ are the two roots of (1). (They cannot be the same root since $\alpha > 0$ and $\frac{-1}{\beta} < 0$.) We can check that this is so by actually solving the equations. The roots of (1) are $\frac{3 \pm \sqrt{30}}{3}$, α being the positive one, whilst the positive root of (2) is $\beta = \frac{3+\sqrt{30}}{7}$. Now $\frac{-1}{\beta} = \frac{-7}{3+\sqrt{30}} = \frac{3-\sqrt{30}}{3}$, as claimed.

The pair of quadratic irrationals $r \pm s\sqrt{d}$ (which are the two roots of some quadratic equation with integer coefficients) are called *algebraic conjugates*. So α and β are related, in that $\frac{-1}{\beta}$ is the algebraic conjugate of α.

SAQ 14 Let $\alpha = [\overline{2;3,5,1}]$ and $\beta = [\overline{1;5,3,2}]$. Show that α and $\frac{-1}{\beta}$ are algebraic conjugates.

SOLUTION TO SAQ 14 The convergents of α are $\frac{2}{1}, \frac{7}{3}, \frac{37}{16}, \frac{44}{19}, \frac{44\alpha+37}{19\alpha+16} = \alpha$, and so

$$19\alpha^2 - 28\alpha - 37 = 0. \tag{1}$$

The convergents of β are $\frac{1}{1}, \frac{6}{5}, \frac{19}{16}, \frac{44}{37}, \frac{44\beta+19}{37\beta+16} = \beta$, and so

$$37\beta^2 - 28\beta - 19 = 0. \tag{2}$$

Substituting $\frac{-1}{\beta}$ for α in (1) gives (2), and so α and $\frac{-1}{\beta}$ are the two (irrational) roots of (1), and as such are algebraic conjugates.

(For the record, α and $\frac{-1}{\beta}$ are the pair $\frac{14 \pm \sqrt{899}}{19}$, but notice that there was no need for us to calculate α and β.) ■

In Example 5 and SAQ 14, the all-important relationship between the coefficients of the quadratic equations in α and β stemmed from a connection between the last pair of convergents of α and β. In Example 5, we had $\frac{14}{5}, \frac{17}{6}$ for α and $\frac{6}{5}, \frac{17}{14}$ for β. In SAQ 14, we had $\frac{37}{16}, \frac{44}{19}$ for α and $\frac{19}{16}, \frac{44}{37}$ for β. This suggests the following general result, which we prove on our way to a classification of those irrational numbers which have a purely periodic continued fraction.

LEMMA Let the final two convergents of $[a_0; a_1, a_2, \ldots, a_n]$ be $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$. Then the final two convergents of $[a_n; a_{n-1}, \ldots, a_1, a_0]$ are $\frac{q_n}{q_{n-1}}$ and $\frac{p_n}{p_{n-1}}$.

PROOF (By mathematical induction on n.)

The case $n = 1$ is easily verified. The only two convergents of $[a_0; a_1]$ are $\frac{a_0}{1}$ and $\frac{a_0 a_1 + 1}{a_1}$, whilst the two convergents of $[a_1; a_0]$ are $\frac{a_1}{1}$ and $\frac{a_0 a_1 + 1}{a_0}$. The pairs are related as claimed.

The inductive step is a little more complicated, but provides good opportunity to practise manipulation of convergents.

SAQ 15 Complete the proof of the Lemma.

SOLUTION TO SAQ 15 Assume the result is true for $n = k$. With the usual notation for convergents this means that the final two convergents of $[a_0; a_1, a_2, \ldots, a_k]$ are $\frac{p_{k-1}}{q_{k-1}}$ and $\frac{p_k}{q_k}$, and the final two convergents of $[a_k; a_{k-1}, \ldots, a_1, a_0]$ are $\frac{q_k}{q_{k-1}}$ and $\frac{p_k}{p_{k-1}}$.

Consider $[a_0; a_1, \ldots, a_k, a_{k+1}]$, whose final two convergents are $\frac{p_k}{q_k}$ and $\frac{p_{k+1}}{q_{k+1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}$. We need to prove that the final two convergents of $[a_{k+1}; a_k, \ldots, a_1, a_0]$ are $\frac{a_{k+1} q_k + q_{k-1}}{q_k}$ and $\frac{a_{k+1} p_k + p_{k-1}}{p_k}$. That is, we must show that

$$[a_{k+1}; a_k, \ldots, a_1] = \frac{a_{k+1} q_k + q_{k-1}}{q_k}$$

and

$$[a_{k+1}; a_k, \ldots, a_1, a_0] = \frac{a_{k+1} p_k + p_{k-1}}{p_k}.$$

Now

$$\begin{aligned} [a_{k+1}; a_k, \ldots, a_2, a_1] &= a_{k+1} + \frac{1}{[a_k; a_{k-1}, \ldots, a_2, a_1]} \\ &= a_{k+1} + \frac{1}{q_k/q_{k-1}} = \frac{a_{k+1} q_k + q_{k-1}}{q_k}. \end{aligned}$$

(Note that $[a_k; a_{k-1}, \ldots, a_2, a_1] = q_k/q_{k-1}$ by the inductive hypothesis, being the penultimate convergent of $[a_k; a_{k-1}, \ldots, a_1, a_0]$.) And

$$\begin{aligned} [a_{k+1}; a_k, \ldots, a_1, a_0] &= a_{k+1} + \frac{1}{[a_k; a_{k-1}, \ldots, a_1, a_0]} \\ &= a_{k+1} + \frac{1}{p_k/p_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{p_k}. \quad \blacksquare \end{aligned}$$

Returning now to our purely periodic continued fraction, we shall establish the general result which we illustrated in Example 5 and SAQ 14.

If $\alpha = \overline{[a_0; a_1, a_2, \ldots, a_n]}$, then (see Example 2) α is the positive root of the quadratic equation $q_n\alpha^2 + (q_{n-1} - p_n)\alpha - p_{n-1} = 0$. Reversing the order of the elements in the cycle of α, we get
$\beta = \overline{[a_n; a_{n-1}, \ldots, a_1, a_0]} = [a_n; a_{n-1}, \ldots, a_1, a_0, \beta]$. By the Lemma, the final three convergents of the latter are $\dfrac{q_n}{q_{n-1}}$, $\dfrac{p_n}{p_{n-1}}$ and $\dfrac{\beta p_n + q_n}{\beta p_{n-1} + q_{n-1}} = \beta$. Hence β is the positive root of $p_{n-1}\beta^2 + (q_{n-1} - p_n)\beta - q_n = 0$. Replacing α by $\dfrac{-1}{\beta}$ in the first of these quadratics gives the second, and so α and $\dfrac{-1}{\beta}$ are algebraic conjugates.

Collecting all this together, noting that $\alpha > 1$ (since $a_0 \geq 1$) and $-\dfrac{1}{\beta} > -1$, we have proved:

THEOREM 1 A purely periodic continued fraction is a quadratic irrational greater than 1 whose algebraic conjugate lies between -1 and 0.

It turns out that the converse of Theorem 1 is also true, but this is a much deeper result, which we are not going to prove here. The first proof was given by Galois in 1828 although, from earlier works, the result seems to have been known to Lagrange.

CONVERSE 1 Any quadratic irrational greater than 1 whose algebraic conjugate lies between -1 and 0 has a purely periodic continued fraction.

As a consequence of Theorem 1 and its converse, we can also classify *all* periodic continued fractions.

THEOREM 2 Any periodic continued fraction is a quadratic irrational.

PROOF Let $y = [a_0; a_1, \ldots, a_n, \overline{b_0, b_1, \ldots, b_m}]$ be periodic. Then $x = \overline{[b_0; b_1, \ldots, b_m]}$ is purely periodic and so, by Theorem 1, x is the positive root of a quadratic $rx^2 + sx + t = 0$, where r, s and t are integers.

Writing $y = [a_0; a_1, \ldots, a_n, x]$, with the usual notation for convergents $y = \dfrac{p_n x + p_{n-1}}{q_n x + q_{n-1}}$, giving $x = \dfrac{q_{n-1}y - p_{n-1}}{p_n - q_n y}$. Substituting this value of x into the quadratic we obtain

$$r\left(\frac{q_{n-1}y - p_{n-1}}{p_n - q_n y}\right)^2 + s\left(\frac{q_{n-1}y - p_{n-1}}{p_n - q_n y}\right) + t = 0$$

or

$$r(q_{n-1}y - p_{n-1})^2 + s(q_{n-1}y - p_{n-1})(p_n - q_n y) + t(p_n - q_n y)^2 = 0$$

which is of the form $Ay^2 + By + C = 0$, where A, B and C are integers. As y must be irrational, this confirms that y is a quadratic irrational, as claimed. ■

The converse of Theorem 2 is also true. Its proof follows without too much difficulty from Converse 1, but again we shall omit it.

CONVERSE 2 Any quadratic irrational has a periodic continued fraction.

In conclusion, let us apply these results to $\sqrt{d}$, where d is a non-square integer, to verify our conjecture of SAQ 13.

$[\sqrt{d}] + \sqrt{d}$ is a quadratic irrational greater than 1 whose algebraic conjugate $[\sqrt{d}] - \sqrt{d}$ satisfies $-1 < [\sqrt{d}] - \sqrt{d} < 0$. Hence, according to Converse 1,

$[\sqrt{d}] + \sqrt{d}$ has a purely periodic continued fraction, say

$$[\sqrt{d}] + \sqrt{d} = [\overline{2a_0; a_1, a_2, \ldots, a_n}],$$

where $a_0 = [\sqrt{d}]$, since the integer part of $[\sqrt{d}] + \sqrt{d}$ is $2[\sqrt{d}]$. Reversing the period gives a continued fraction whose value is minus the reciprocal of the algebraic conjugate of $[\sqrt{d}] + \sqrt{d}$. That is,

$$[\overline{a_n; a_{n-1}, \ldots, a_1, 2a_0}] = \frac{-1}{a_0 - \sqrt{d}} = \frac{1}{\sqrt{d} - a_0}. \qquad (1)$$

But

$$\sqrt{d} + a_0 = 2a_0 + (\sqrt{d} - a_0) = 2a_0 + \frac{1}{\left(\dfrac{1}{\sqrt{d} - a_0}\right)}$$

and

$$\sqrt{d} + a_0 = [\overline{2a_0; a_1, \ldots, a_n}] = 2a_0 + \frac{1}{[\overline{a_1; a_2, \ldots, a_n, 2a_0}]}.$$

Therefore

$$\frac{1}{\sqrt{d} - a_0} = [\overline{a_1; a_2, \ldots, a_n, 2a_0}]. \qquad (2)$$

By the uniqueness of continued fractions, comparison of the expressions (1) and (2) for $\dfrac{1}{\sqrt{d} - a_0}$ gives $a_1 = a_n$, $a_2 = a_{n-1}$, etc., establishing the symmetric property of the period.

Collating this information.

$$[\sqrt{d}] + \sqrt{d} = [\overline{2a_0; a_1, a_2, \ldots, a_2, a_1}]$$

or, equivalently,

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}].$$

SAQ 16 Which of the following quadratic irrationals have a purely periodic continued fraction?

(a) $\dfrac{2 + 6\sqrt{7}}{5}$, (b) $\dfrac{1 + \sqrt{37}}{6}$, (c) $-7 - 2\sqrt{11}$.

SOLUTION TO SAQ 16

(a) $\dfrac{2 + 6\sqrt{7}}{5}$ does not have a purely periodic continued fraction because its algebraic conjugate, $\dfrac{2 - 6\sqrt{7}}{5}$, is less than -1.

(b) $\dfrac{1 + \sqrt{37}}{6} > 1$ and its algebraic conjugate satisfies $-1 < \dfrac{1 - \sqrt{37}}{6} < 0$, so it has a purely periodic continued fraction.

(c) Although the algebraic conjugate $-7 + 2\sqrt{11}$ lies between -1 and 0, since $-7 - 2\sqrt{11}$ is not greater than 1, it does not have a purely periodic continued fraction. ■

7.5 Rational Approximations

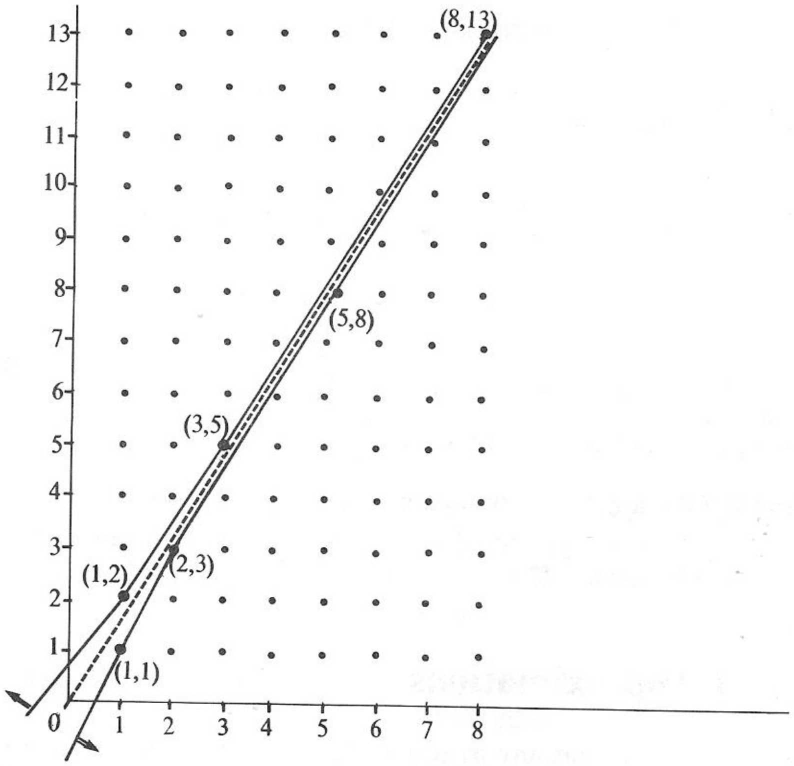
So far we have seen that any irrational number has a unique infinite continued fraction and that we obtain a sequence of rational approximations to the irrational number by taking the convergents. We even have an estimate for how good these approximations are. However, we have not yet fulfilled the promise made in the introduction that the continued fraction provides what are, in some sense, best possible rational approximations.

Given an irrational number x, we can always improve on any rational approximation $\frac{a}{b}$. In fact, there are infinitely many rational numbers lying between $\frac{a}{b}$ and x. Consequently there is no such thing as *the best* rational approximation to x. However, if we impose restrictions on the size of the denominator, we can ask about the best rational approximation to x. For example, of all rational numbers whose (positive) denominator does not exceed 50, the best approximation to π is $\frac{22}{7}$. (To improve on $\frac{22}{7}$ we have to go to $\frac{179}{57}$.) We shall show that if p_n/q_n is any convergent of x, then there is *no* rational number a/b with $0 < b \leq q_n$ which approximates x better than p_n/q_n and in this sense the convergents of x are best rational approximations to it.

Before embarking on the reading passage we must give you a beautiful geometric interpretation of the continued fraction for an irrational number, which was first given by Klein in 1895. It illustrates precisely the sense in which convergents are best rational approximations.

Let α be a positive irrational number and consider the part of the line $y = \alpha x$ in the first quadrant of the Cartesian plane. This line cannot pass through any of the lattice points (i.e. points whose coordinates are both integers) except $(0, 0)$, for if it did, α would be rational. Imagine that pins are set upright at each of the lattice points in the first quadrant, and a fine string is placed along the line with one end fixed to the line at an infinitely remote point, and the other end at the origin. Keeping the string tight we move the end at the origin towards the right. It will catch on a series of pins below the line. In fact, the pins on which it catches are those at lattice points with coordinates (q_0, p_0), (q_2, p_2), $(q_4, p_4), \ldots$ corresponding to the even convergents p_0/q_0, p_2/q_2, $p_4/q_4, \ldots$ of α.

Similarly, if we move the string from the origin to the left it catches on pegs at (q_1, p_1), (q_3, p_3), $(q_5, p_5), \ldots$ corresponding to the odd convergents p_1/q_1, p_3/q_3, $p_5/q_5, \ldots$ of α.



The figure shows this for the case $\alpha = \dfrac{1 + \sqrt{5}}{2}$, the golden ratio, whose convergents are $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots$. The dashed line is the portion of $y = \alpha x$ in the first quadrant. Moving to the right it catches on the pins with coordinates $(1, 1)$, $(2, 3)$, $(5, 8), \ldots$ whilst moving left it catches on the pins at $(1, 2)$, $(3, 5)$, $(8, 13), \ldots$.

So much for the preview. The proof of the first Lemma in the reading passage is somewhat involved, but once that is out of the way the rest is plain sailing.

READ B from page 323, line 10 to page 325, line 10.

SAQ 17 (a) Prove that the convergents of x (irrational) are successively closer to x. That is,

$$\left|x-\frac{p_{n+1}}{q_{n+1}}\right| < \left|x-\frac{p_n}{q_n}\right|.$$

(b) Prove that the convergents of x satisfy

$$\frac{1}{2q_nq_{n+1}} < \left|x-\frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}.$$

SOLUTION TO SAQ 17 (a) This is an immediate consequence of Theorem 13-12. Since the q_k are increasing, $q_n \le q_{n+1}$ and so

$$\left|x-\frac{p_{n+1}}{q_{n+1}}\right| \le \left|x-\frac{p_n}{q_n}\right|.$$

Equality cannot occur, for if it did, we would have

$$x-\frac{p_{n+1}}{q_{n+1}} = \frac{p_n}{q_n}-x \qquad \text{(since } x \text{ lies between successive convergents)}$$

which leads to $x = \frac{1}{2}\left(\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right)$, contradicting the irrationality of x.

(b) The right-hand part of the inequality is the Corollary on page 320 of **B**. For the left-hand part, note that

$$\frac{1}{q_nq_{n+1}} = \left|\frac{p_n}{q_n}-\frac{p_{n+1}}{q_{n+1}}\right| = \left|x-\frac{p_n}{q_n}\right| + \left|x-\frac{p_{n+1}}{q_{n+1}}\right|$$

(since $|p_nq_{n+1}-p_{n+1}q_n| = 1$ and $x-\frac{p_n}{q_n}$, $x-\frac{p_{n+1}}{q_{n+1}}$ have opposite signs).

Now, using part (a),

$$\frac{1}{q_nq_{n+1}} < 2\left|x-\frac{p_n}{q_n}\right|$$

which gives the required inequality. ■

The final reading passage provides us with a test for whether a rational approximation to x will occur as one of its convergents.

READ B from page 325, line 11 to the end of Section 13.4.

SAQ 18 **B** page 328, Problems 13.4, number 10.

SOLUTION TO SAQ 18

$$\frac{1+\sqrt{10}}{3}-\frac{18}{13} = \frac{13\sqrt{10}-41}{39} = \frac{3}{13(13\sqrt{10}+41)} \qquad (\text{since } 13^2\cdot 10 - 41^2 = 9).$$

Now $\sqrt{10} > 3$, and so $\frac{1+\sqrt{10}}{3}-\frac{18}{13} < \frac{3}{13\cdot 80} < \frac{1}{2\cdot 13^2}$.

Theorem 13-13 establishes that $\frac{18}{13}$ is a convergent of $\frac{1+\sqrt{10}}{3}$.

For verification, $\frac{1+\sqrt{10}}{3}$ has continued fraction $[1;\overline{2,1,1}]$ which has convergents $\frac{1}{1}, \frac{3}{2}, \frac{4}{3}, \frac{7}{5}, \frac{18}{13}, \ldots$. ■

7.6 Summary

In this unit we have studied continued fractions and some of their properties. We started by investigating finite continued fractions, many of whose properties were important for the subsequent development of the infinite continued fraction. We saw how to use the Division Algorithm to obtain a continued fraction for any rational number, and a generalization of this technique, the Continued Fraction Algorithm, led us to the unique infinite continued fraction of an irrational number.

One of the themes of the unit was to classify the numbers associated with various kinds of continued fraction. To this end we saw that rational numbers correspond to finite continued fractions, irrational numbers to infinite continued fractions and quadratic irrationals to periodic continued fractions. The latter category was broken down further by classifying which quadratic irrationals correspond to the purely periodic continued fractions. We also found the particular form of the continued fraction of $\sqrt{d}$, where d is any non-square integer.

We discovered a good method, based on continued fractions, for solving linear Diophantine equations. (In *Unit 8* we shall use continued fractions to solve another family of Diophantine equations.)

One of the main applications of continued fractions is in the area of finding rational approximations to irrationals. We discovered that the convergents of an irrational number are, in a certain sense, best rational approximations.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

UNIT 8

DIOPHANTINE EQUATIONS

8.0 Introduction

Our first encounter with a Diophantine equation was in *Unit 1*, where we were confronted with the linear Diophantine equation $ax + by + c = 0$. Prior to this course, you would have probably associated with this equation the geometric picture of a straight line in the plane, and the solution set of the equation consisting of those ordered pairs of real numbers (x, y) corresponding to points on the line. But in number theory we restrict ourselves to the integers, rather than real numbers, so the solutions we require are the ordered pairs of integers (x, y) which satisfy the equation. Geometrically, we seek the lattice points which the line $ax + by + c = 0$ passes through. There are a number of questions that we can ask, and have asked, of the linear Diophantine equation:

(i) Are there any integer solutions?

(ii) Is the set of integer solutions infinite?

(iii) Is there a method of finding all integer solutions?

We had little difficulty supplying answers to all three questions for the linear Diophantine equation. But the same questions can be asked of any polynomial equation $P(x_1, x_2, \ldots, x_n) = 0$ in n variables, and, more often than not, these questions present considerable difficulty, even when $n = 2$ and P is a fairly simple polynomial. For example, consider $x^3 - y^2 = 2$. You might be able to answer question (i) by spotting a solution, but how about questions (ii) and (iii)? (Fermat managed it, but we shall not go into his solution here.)

Questions of this nature are called Diophantine problems, named after Diophantus of Alexandria, who initiated their study through several problems involving squares and cubes which arose out of geometrical considerations.

Number theory is a vast subject, and there are many branches which we have not touched upon in this course. However, nearly all branches have as their motivation the objective of making a contribution to the solution of one or more Diophantine equations. It is this topic of Diophantine equations which, historically, lies at the heart of number theory, and the study of which has, over the ages, stimulated to a considerable extent the development of mathematical thought.

In this unit we are going to look at a handful of the many notorious Diophantine equations, each one of which, as you will read, is surrounded by its own fascinating history. The material is selected from **B**, Chapters 11, 12 and 13.

In Section 8.1 we continue where we left *Unit 7*, looking at an application of continued fractions. We shall find that Pell's Equation, $x^2 - dy^2 = 1$, where the positive integer d is not a square, has infinitely many solutions, all of which are readily obtained from the continued fraction of $\sqrt{d}$.

Section 8.2 investigates the Pythagorean equations. Perhaps the best known theorem in the whole of mathematics is that of Pythagoras, which says that if x, y and z are the lengths of the sides of a right-angled triangle, z being the length of the hypotenuse, then $x^2 + y^2 = z^2$. Solving this as a Diophantine equation amounts to finding all right-angled triangles whose side lengths are integers.

Section 8.3 turns to the equations $x^n + y^n = z^n$, for $n > 2$. These equations hold a prominent place in mathematics because of the history surrounding unsuccessful attempts to show that they have no solutions (other than the trivial ones in which x or y is equal to 0). The conjecture that they have no solutions has become known as Fermat's Last Theorem. We shall use our solution to the Pythagorean equation to prove Fermat's Last Theorem for the special case $n = 4$. This proof involves us in the one new technique of this unit: Fermat's method of infinite descent.

Finally, Section 8.4 looks at the problem of representing integers as sums of squares. We shall give a complete solution of the two squares problem, that is, we shall classify those integers N for which the Diophantine equation $x^2 + y^2 = N$ has solutions. The section rounds off with a brief look at the allied three squares and four squares problems and includes the result that every positive integer is a sum of four squares.

8.1 Pell's Equation

We start our survey of Diophantine equations with one which has a curious history, Pell's equation $x^2 - dy^2 = 1$, where the positive integer d is a non-square.

As $\sqrt{d}$ is irrational, the equation $\frac{x^2}{y^2} = d$, i.e. $x^2 - dy^2 = 0$, has no integer solutions. But if $\frac{x}{y}$ is a good rational approximation to $\sqrt{d}$, then $\frac{x^2}{y^2}$ will be relatively close to d, or what amounts to the same thing, $x^2 - dy^2 = k$ will be a small integer. As k cannot equal 0, the next best thing is that $k = \pm 1$. Having seen that the convergents of the continued fraction of $\sqrt{d}$ are 'best' rational approximations, it will come as no surprise to discover that every solution (x, y) of either of the equations $x^2 - dy^2 = \pm 1$ arises as a convergent $\frac{x}{y}$ of $\sqrt{d}$.

The bulk of the first reading passage is concerned with the origins of Pell's equation.

READ B Section 13.5, page 329 as far as the bottom of page 333.

SAQ 1 **B** page 341, Problems 13.5, number 3.

SOLUTION TO SAQ 1 Knowing that all solutions are to be found amongst the convergents of the continued fraction of $\sqrt{d}$, we need check, in each case, only those convergents with denominator less than 250.

(a) $x^2 - 2y^2 = 1$

The continued fraction for $\sqrt{2}$ is $[1;\overline{2}]$ and so the convergents are $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \ldots$. All subsequent ones have denominator exceeding 250. The corresponding values of $p_n^2 - 2q_n^2$ are, respectively, $-1, 1, -1, 1, -1, 1, -1, \ldots$, and so the required solutions are (3, 2), (17, 12) and (99, 70).

COMMENT Note how we can use Theorem 13-15 to assist in calculating $p_n^2 - 2q_n^2$. It tells us that $|p_n^2 - 2q_n^2| < 1 + 2\sqrt{2} < 4$, and so we need only look at the units digit of $p_n^2 - 2q_n^2$. For example, for the convergent $\frac{239}{169}$,

$$239^2 - 2 \cdot 169^2 \equiv 9^2 - 2 \cdot 9^2 \equiv 1 - 2 \cdot 1 \equiv -1 \equiv 9 \pmod{10}$$

and so we must have $239^2 - 2 \cdot 169^2 = -1$.

(b) $x^2 - 3y^2 = 1$

The continued fraction for $\sqrt{3}$ is $[1;\overline{1,2}]$, and the convergents with denominator $q_n < 250$ are $\frac{1}{1}, \frac{2}{1}, \frac{5}{3}, \frac{7}{4}, \frac{19}{11}, \frac{26}{15}, \frac{71}{41}, \frac{97}{56}, \frac{265}{153}$ and $\frac{362}{209}$. The corresponding values of $p_n^2 - 3q_n^2$ are respectively $-2, 1, -2, 1, -2, 1, -2, 1, -2$ and 1, and the required solutions are (2, 1), (7, 4), (26, 15), (97, 56) and (362, 209).

(c) $x^2 - 5y^2 = 1$

From the continued fraction $\sqrt{5} = [2;\overline{4}]$, the convergents of $\sqrt{5}$ are $\frac{2}{1}, \frac{9}{4}, \frac{38}{17}, \frac{161}{72}, \ldots$, with corresponding values of $p_n^2 - 5q_n^2$ being $-1, 1, -1, 1, \ldots$. The required solutions are (9, 4) and (161, 72). ■

We now know that any solution of Pell's equation $x^2 - dy^2 = 1$ must arise as the numerator and denominator of a convergent of $\sqrt{d}$. What is more, in each of the examples, we have seen that solutions always occurred. Will this be true of every non-square positive integer d, and, if so, which convergents provide the solutions? Answers to both these questions are to be found in the next reading passage.

READ B from the top of page 335 to page 337, line 3.

NOTES (i) *Page 335 line 10*

The Lemma tells us which convergents can provide the solutions of Pell's equation. They are the convergents which immediately precede the partial denominator $2a_0$ at the end of the period of the continued fraction for $\sqrt{d}$:

$$\begin{aligned}\sqrt{d} &= [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]\\ &= [a_0; a_1, a_2, \ldots, a_2, \underset{\uparrow}{a_1}, 2a_0, a_1, a_2, \ldots, \underset{\uparrow}{a_1}, 2a_0, a_1, \ldots, \underset{\uparrow}{a_1}, 2a_0, \ldots].\end{aligned}$$

The convergents corresponding to the arrowed partial denominators are $\dfrac{p_{kn-1}}{q_{kn-1}}$, $k = 1, 2, 3, \ldots$, where n is the length of the period. If n is even, the Lemma will tell us that $p_{kn-1}^2 - d\,q_{kn-1}^2 = 1$, giving a solution of Pell's equation for every positive integer k. On the other hand, if n is odd the Lemma gives $p_{kn-1}^2 - d\,q_{kn-1}^2 = (-1)^k$, so that we have solutions for $k = 2, 4, 6, \ldots$; whilst for each odd value of k, the convergent gives a solution of $x^2 - dy^2 = -1$.

(ii) *Page 336, line −8*

Remember that the list above starts with $C_0 = p_0/q_0$, and so p_3/q_3 is the fourth in the given list.

(iii) *Page 337, line 3*

In Example 13-8, as the period of $\sqrt{13}$ has odd length, 5, it is only every tenth convergent, $\dfrac{p_9}{q_9}, \dfrac{p_{19}}{q_{19}}, \dfrac{p_{29}}{q_{29}}, \ldots$, which satisfies $p_i^2 - 13q_i^2 = 1$. However, the Lemma on page 335 tells us that every tenth convergent, $\dfrac{p_4}{q_4}, \dfrac{p_{14}}{q_{14}}, \dfrac{p_{24}}{q_{24}}, \ldots$, satisfies $p_i^2 - 13q_i^2 = -1$. We can confirm that this is so for the fourth convergent $\frac{18}{5}$: $18^2 - 13 \cdot 5^2 = -1$. ▲

SAQ 2 **B** page 341, Problems 13.5, number 5.

SAQ 3 **B** page 341, Problems 13.5, number 4.

SAQ 4 **B** page 341, Problems 13.5, number 9.

SOLUTION TO SAQ 2 (a) $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$

As the length of the period is 4, which is even, solutions of Pell's equation are given by convergents $\dfrac{p_{4k-1}}{q_{4k-1}}$, for all $k \geq 1$. The solutions we require will come from p_3/q_3 and p_7/q_7. The convergents are

$$\frac{4}{1}, \frac{5}{1}, \frac{19}{4}, \frac{24}{5}, \frac{211}{44}, \frac{235}{49}, \frac{916}{191}, \frac{1151}{240}, \ldots .$$

So solutions are $(24, 5)$ and $(1151, 240)$.

(Check: $24^2 - 23 \cdot 5^2 = 1$ and $1151^2 - 23 \cdot 240^2 = 1$.)

(b) $\sqrt{26} = [5; \overline{10}]$
The period has odd length, 1, so the solutions to Pell's equation are given by the convergents $\frac{p_{2k-1}}{q_{2k-1}}$, for all $k \geq 1$. The first two solutions come from $\frac{p_1}{q_1} = \frac{51}{10}$ (check: $51^2 - 26 \cdot 10^2 = 1$), and $\frac{p_3}{q_3} = \frac{5201}{1020}$ (check: $5201^2 - 26 \cdot 1020^2 = 1$).

(c) $\sqrt{33} = [5; \overline{1, 2, 1, 10}]$
The period length is 4 (even), so the first two solutions are p_3/q_3 and p_7/q_7. The convergents of $\sqrt{33}$ are $\frac{5}{1}, \frac{6}{1}, \frac{17}{3}, \frac{23}{4}, \frac{247}{43}, \frac{270}{47}, \frac{787}{137}, \frac{1057}{184}, \ldots$. So solutions are $(23, 4)$ and $(1057, 184)$.

(Check: $23^2 - 33 \cdot 4^2 = 1$ and $1057^2 - 33 \cdot 184^2 = 1$.) ■

SOLUTION TO SAQ 3 Suppose $n + 1 = x^2$ and $\frac{n}{2} + 1 = y^2$. Eliminating n from this pair of simultaneous equations gives $x^2 - 2y^2 = -1$. Conversely, if $x^2 - 2y^2 = -1$, then x^2 is odd and therefore can be written as $x^2 = n + 1$, where n is even. Solving for y gives $y^2 = \frac{n}{2} + 1$. Since $\sqrt{2} = [1; \overline{2}]$ has period of odd length, the Lemma on **B** page 335 guarantees infinitely many solutions (arising from the even convergents). The first solutions are $(1, 1)$ giving $n = 0$, $(7, 5)$ giving $n = 48$ and $(41, 29)$ giving $n = 1680$. ■

SOLUTION TO SAQ 4 If $p \mid d$ then $x^2 - dy^2 = -1$ implies that $x^2 \equiv -1 \pmod{p}$. But -1 is not a quadratic residue of $p \equiv 3 \pmod 4$, and so no such x can exist. ■

On pages 337–9, **B** sets up a method by which all solutions of Pell's equation can be generated from the least positive solution. We leave this as optional reading. However, to conclude the section,

READ B page 340.

8.2 The Pythagorean Equation

You will be familiar with the fact that there is a right-angled triangle with sides of lengths 3, 4 and 5 (inches, say), which in terms of the celebrated Pythagoras' Theorem says that $3^2 + 4^2 = 5^2$. This provides us with a first solution of the Diophantine equation

$$x^2 + y^2 = z^2 \tag{1}$$

In this section we are going to find all solutions of this equation. We shall overlook the trivial solutions in which x or y is equal to zero, and, as $x^2 = x^2 = (-x)^2$ etc., we shall concentrate on solutions in which x, y and z are positive, since all other solutions are given by simple changes of sign.

The forementioned solution leads immediately to infinitely many solutions of (1), since for any integer $k \geq 1$,

$$(3k)^2 + (4k)^2 = (5k)^2.$$

Yet, in a sense, all these solutions are 'essentially the same'—geometrically, the corresponding right-angled triangles are all similar. For this reason we attack the Diophantine equation (1) by first looking for positive solutions in which gcd $(x,y,z) = 1$. If we can find all such solutions, then all remaining positive solutions are found, as illustrated above, by multiplying each of the x, y and z values by any integer $k \geq 1$.

READ B Section 11.1, page 242 as far as page 247, line -6.

NOTES (i) *Page 243, line 16*

As we can confine ourselves reasonably to the positive solutions of the Pythagorean equation, we shall also insist that the three integers in a primitive Pythagorean triple are positive.

(ii) *Page 244, line 13*

In any primitive triple, exactly one of x and y is even. Notice that if $x^2 + y^2 = z^2$ then $y^2 + x^2 = z^2$ so that the values of x and y are interchangeable. To overcome this ambiguity, we adopt the convention that x takes the even value in any primitive triple. Note this convention carefully since it will be employed many times in what follows.

(iii) *Page 244, line -13*

Having seen that in any primitive triple x is even, for it to be prime requires that $x = 2$. But we can easily show that there is no such triple, for

$$2^2 + y^2 = z^2$$

gives $4 = (z - y)(z + y)$.

As y and z are known to be odd, $z - y$ and $z + y$ are both even positive integers, giving $z - y = 2$ and $z + y = 2$. That is, $z = 2$, $y = 0$—a contradiction.

On the next line, **B** is technically correct but has overlooked his convention that x is always even. He should say: 'there are primitive triples in which y and z are prime'.

There is overwhelming numerical evidence supporting the conjecture that there are infinitely many such triples, but, like so many similar situations that we have encountered in the course, this still awaits a general proof.

(iv) *Page 245, line 5*

The proof of Lemma 2 is completed more easily by using the result of SAQ 4 of *Unit 2*, which says that an integer is an nth power if and only if each exponent in its prime factorization is a multiple of n. Since ab is an nth power each of its exponents $k_1, \ldots, k_r, j_1, \ldots, j_s$ is a multiple of n, and the expressions for a and b at the foot of page 244 confirm that they are indeed nth powers.

(v) *Page 246, line -5*

The result of Theorem 11-1 amounts to a complete classification of the primitive Pythagorean triples with x even. To get all positive solutions of the Pythagorean equation we drop the condition gcd $(x, y, z) = 1$, and have

$$x = 2kst, \quad y = k(s^2 - t^2), \quad z = k(s^2 + t^2)$$

for any integer $k \geq 1$, observing that x and y are interchangeable. ▲

SAQ 5 **B** page 249, Problems 11.1, number 1.

SAQ 6 Show that in any solution of $x^2 + y^2 = z^2$ at least one of x, y or z is a multiple of 5. Hence solve:

B page 249, Problems 11.1, number 4.

SAQ 7 Show that if p is an odd prime, then $x^2 + y^2 = z^2$ has exactly one positive solution with $y = p$.

SAQ 8 (i) Show that if N, a and b are positive integers such that $N = ab$, then, for any integers s and t,

$$x = as^2 - bt^2, \quad y = 2st, \quad z = as^2 + bt^2$$

is a solution of $x^2 + Ny^2 = z^2$.

(ii) There are six positive solutions of $x^2 + 6y^2 = z^2$ in which $z < 20$; find them.

SOLUTION TO SAQ 5 (a) Theorem 11-1 tells us that primitive solutions are given by

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2 + t^2$$

where $\gcd(s, t) = 1$, $s > t > 0$ and $s \not\equiv t \pmod 2$. Given that $x = 16$, the only primitive solution arises from $s = 8$, $t = 1$, whence $x = 16$, $y = 63$ and $z = 65$.

We can find solutions which are not primitive by the same method but solving for x being a divisor of 16.

$$s = 4, t = 1 \quad \text{gives} \quad x = 8, y = 15, z = 17.$$

Multiplying by 2 gives the solution $x = 16$, $y = 30$, $z = 34$.

$$s = 2, t = 1 \quad \text{gives} \quad x = 4, y = 3, z = 5.$$

Multiplying by 4 gives the solution $x = 16$, $y = 12$, $z = 20$.

(b) For $x = 40$ we require all pairs of positive values of s and t $(s > t)$ such that $2st = 40$, $\gcd(s, t) = 1$, $s \not\equiv t \pmod 2$. They are

$$s = 20, t = 1 \quad \text{giving} \quad x = 40, y = 399, z = 401,$$

and

$$s = 5, t = 4 \quad \text{giving} \quad x = 40, y = 9, z = 41.$$

For $x = 60$, proceding similarly,

$$s = 30, t = 1 \quad \text{giving} \quad x = 60, y = 899, z = 901,$$

$$s = 15, t = 2 \quad \text{giving} \quad x = 60, y = 221, z = 229,$$

$$s = 10, t = 3 \quad \text{giving} \quad x = 60, y = 91, \quad z = 109,$$

$$s = 6, \quad t = 5 \quad \text{giving} \quad x = 60, y = 11, \quad z = 61. \quad ■$$

SOLUTION TO SAQ 6 If $x^2 + y^2 = z^2$, suppose that $5 \nmid x$ and $5 \nmid y$. We must show that $5 | z$.

Since $5 \nmid x$, $x^2 \equiv 1$ or $4 \pmod 5$ and similarly $y^2 \equiv 1$ or $4 \pmod 5$. Therefore

$$x^2 + y^2 \equiv \{1 \text{ or } 4\} + \{1 \text{ or } 4\} \pmod 5$$

$$\equiv 0, 2 \text{ or } 3 \pmod 5.$$

But 2 and 3 are not quadratic residues of 5 and so we must have $z^2 \equiv 0 \pmod 5$, which amounts to $5 | z$.

To prove that $60 | xyz$, we show that $3 | xyz$, $4 | xyz$ and $5 | xyz$, and appeal to Corollary 2 on **B** page 28, observing that 3, 4 and 5 are pairwise relatively prime with product equal to 60. In fact, we have just shown that $5 | xyz$ and on page 247 of **B** we saw that $3 | x$ or $3 | y$, yielding $3 | xyz$. So it remains to show only that $4 | xyz$. For this we need only look at the form of x in any primitive solution. By Theorem 11-1, $x = 2st$ where $s \not\equiv t \pmod 2$. The latter fact forces one of s or t to be even, and in turn $4 | x$. Therefore $4 | xyz$, as required. ■

SOLUTION TO SAQ 7

Suppose there is a solution with $y = p$. Then from $x^2 + p^2 = z^2$ we have

$$p^2 = z^2 - x^2 = (z - x)(z + x).$$

Now x and z are both positive and $z > x$, so $z + x > z - x > 0$. As p^2 can be expressed as a product of two positive integers in only two ways, namely $1 \cdot p^2$ and $p \cdot p$ we conclude that

$$z - x = 1 \text{ and } z + x = p^2.$$

(That both should be equal to p is excluded since $z + x > z - x$.) From these two equations we conclude that

$$x = \frac{1}{2}(p^2 - 1) \quad \text{and} \quad z = \frac{1}{2}(p^2 + 1).$$

So any solution with $y = p$ is uniquely determined. On the other hand, it is a simple matter to verify that

$$x = \frac{1}{2}(p^2 - 1),\ y = p,\ z = \frac{1}{2}(p^2 + 1)$$

is a primitive Pythagorean triple, for any odd prime p.

COMMENTS

1. In fact, it is not difficult to show (from Theorem 11-1) that not only odd primes, but every integer $n > 1$ (provided $n \not\equiv 2 \pmod 4$) occurs in some primitive Pythagorean triple. The reason why $n \equiv 2 \pmod 4$ is excluded was seen in SAQ 6, where we found that the even member in any primitive Pythagorean triple is always divisible by 4.
2. If $z = \frac{1}{2}(p^2 + 1)$ is prime then we have found a primitive Pythagorean triple with y and z both prime. We commented in Note (iii) that it is not known whether there are infinitely many such triples. Our solution therefore brings to the fore yet another unsolved problem: are there infinitely many pairs of primes p and q such that $2q = p^2 + 1$? ■.

SOLUTION TO SAQ 8

(i) This part is just algebraic manipulation:

$$\begin{aligned} x^2 + Ny^2 &= (as^2 - bt^2)^2 + ab(2st)^2 \\ &= a^2s^4 + 2abs^2t^2 + b^2t^4 \\ &= (as^2 + bt^2)^2 \\ &= z^2. \end{aligned}$$

(ii) For $N = 6$ we have the two cases $a = 6$, $b = 1$ and $a = 3$, $b = 2$ to consider. (The cases $a = 1$, $b = 6$ and $a = 2$, $b = 3$ will lead to the same solutions but with a change of sign in the x-value.)

With $a = 6$ and $b = 1$, $z = 6s^2 + t^2 < 20$ requires $s = 0$ or 1. However, $s = 0$ will give $y = 2st = 0$, so we are left with $s = 1$, in which case $t = 1$, 2 or 3:

$$\begin{aligned} s = 1, t = 1 \quad &\Rightarrow \quad x = 5, y = 2, z = 7, \\ s = 1, t = 2 \quad &\Rightarrow \quad x = 2, y = 4, z = 10, \\ s = 1, t = 3 \quad &\Rightarrow \quad x = -3, y = 6, z = 15. \end{aligned}$$

As the sign of x is immaterial, since it is to be squared, the last gives us the positive solution $x = 3$, $y = 6$, $z = 15$.

With $a = 3$ and $b = 2$, $z = 3s^2 + 2t^2 < 20$ gives us three cases:

$$s = 1, t = 1 \quad \Rightarrow \quad x = 1, y = 2, z = 5,$$

$$s = 1, t = 2 \quad \Rightarrow \quad x = -5, y = 4, z = 11$$

(this gives the positive solution $x = 5$, $y = 4$, $z = 11$),

$$s = 2, t = 1 \quad \Rightarrow \quad x = 10, y = 4, z = 14. \quad ■$$

8.3 Fermat's Last Theorem

In this section we shall read more about the history and the present state of play of attempts to prove Fermat's Last Theorem. We shall also see a proof for the particular case $n = 4$. In that proof, we shall encounter an important and powerful technique known as 'Fermat's method of infinite descent'. It is used here to show the non-existence of solutions of particular Diophantine equations. In Section 8.4, however, we shall use the descent method in a slightly different way to establish the existence of solutions of certain other Diophantine equations.

As we shall use it in this section, the idea behind the descent method is as follows. We suppose that the Diophantine equation in question has a positive solution. Then, focussing on one of the variables involved, say z, the Well Ordering Principle tells us that amongst all solutions there is one in which z takes its least positive value. We contradict this by showing, by some algebraic argument, that any solution of the Diophantine equation gives rise to a second solution in which the positive value of z has decreased. (This key stage of the method is called the *descent step.*) The only conclusion to be drawn is that the set to which we have applied the Well Ordering Principle must be empty. That is, the Diophantine equation has no positive solutions.

The application of the descent method in the reading passage is quite involved, but in the SAQs at the end of the section we have given you two simpler Diophantine problems which can be solved by this method.

READ B Section 11.2, page 250 as far as page 254, line 16.

NOTES

(i) *Page 251, line 4*
Since $x_0 = dx_1$ and $y_0 = dy_1$ we have $x_0^4 + y_0^4 = d^4(x_1^4 + y_1^4) = z_0^2$. From this it follows that $d^2 | z_0$, which justifies putting $z_0 = d^2 z_1$.

(ii) *Page 251, line 19*
$1 \equiv y_0^2 \pmod 4$ follows since y_0 is presumed to be odd and the square of any odd integer is congruent to 1 modulo 4.

(iii) *Page 254, line 16*
It is said that the great number theorist Landau had postcards printed which read: 'Dear Sir or Madam: Your attempted proof of Fermat's Theorem has been received and is returned herewith. The first mistake is on page , line .' Landau left to his students the task of filling in the missing numbers. ▲

SAQ 9 **B** page 258, Problems 11.2, number 12.

SAQ 10 Use the method of infinite descent to show that

$$x^3 + 3y^3 = 9z^3$$

has no positive solutions. (Hint: In any solution, $3 | x$.)

SAQ 11 Show that if $x^2 + y^2 + z^2 \equiv 0 \pmod 4$, then each of x, y and z is even. Hence use the method of infinite descent to show that

$$x^2 + y^2 + z^2 = 2xyz$$

has no solutions other than $x = y = z = 0$.

SAQ 12 [Hard] **B** page 258, Problems 11.2, number 7. (Hint: The hint in **B** provides the final step of the argument but it is far from clear how one arrives at his expressions for $x^2 + y^2$, $x + y$ and $x - y$. Observing that the product of these three terms is $x^4 - y^4$, Lemma 2 (**B** page 244) will give us the expressions, provided the three factors are pairwise relatively prime. For that we first need $\gcd(x, y) = 1$.)

SOLUTION TO SAQ 9 $\dfrac{1}{x^4} + \dfrac{1}{y^4} = \dfrac{1}{z^2}$ rearranges to $x^4 + y^4 = \left(\dfrac{x^2y^2}{z}\right)^2$, and Theorem 11-3 tells us that this equation has no solutions in positive integers. ■

SOLUTION TO SAQ 10 Suppose we have a positive solution x_0, y_0, z_0 so that

$$x_0^3 + 3y_0^3 = 9z_0^3.$$

Now $x_0^3 = 3(3z_0^3 - y_0^3)$, showing that $3 \mid x_0$. Putting $x_0 = 3x_1$,

$$27x_1^3 + 3y_0^3 = 9z_0^3, \quad \text{or} \quad 9x_1^3 + y_0^3 = 3z_0^3.$$

But now $3 \mid y_0$ and so, putting $y_0 = 3y_1$,

$$9x_1^3 + 27y_1^3 = 3z_0^3, \quad \text{or} \quad 3x_1^3 + 9y_1^3 = z_0^3.$$

This time $3 \mid z_0$, and putting $z_0 = 3z_1$ gives

$$3x_1^3 + 9y_1^3 = 27z_1^3, \quad \text{or} \quad x_1^3 + 3y_1^3 = 9z_1^3.$$

This completes the descent step. Any positive solution gives rise to a another solution in which the value of each of the variables has decreased, for example $0 < x_1 = \dfrac{x_0}{3} < x_0$. Hence, by the method of infinite descent, the Diophantine equation has no positive solutions.

COMMENT In this example we could avoid appealing to the method of infinite descent. Assuming the existence of a solution, cancellation of all common factors would give a solution with $\gcd(x, y, z) = 1$. The above argument produces a contradiction by showing that $\gcd(x, y, z) \geq 3$. ■

SOLUTION TO SAQ 11 $a^2 \equiv 0$ or $1 \pmod 4$ according as a is even or odd respectively. So

$$\begin{aligned} x^2 + y^2 + z^2 &\equiv (0 \text{ or } 1) + (0 \text{ or } 1) + (0 \text{ or } 1) \pmod 4 \\ &\equiv 0,\ 1,\ 2 \text{ or } 3 \pmod 4 \end{aligned}$$

according as none, one, two, or three, respectively, of x, y and z are odd. So $x^2 + y^2 + z^2 \equiv 0 \pmod 4$ precisely when x, y and z are all even.

In looking for solutions of $x^2 + y^2 + z^2 = 2xyz$, we assume that x, y and z are positive, since all other non-trivial solutions are given by simple changes of sign.

If x, y and z are all odd then $x^2 + y^2 + z^2 \equiv 3 \pmod 4$ whilst $2xyz \equiv 2 \pmod 4$. So at least one of x, y and z is even, and now $2xyz \equiv 0 \pmod 4$. By the first part of the question, it follows that x, y and z must all be even. Therefore, writing $x = 2x'$, $y = 2y'$ and $z = 2z'$, we have

$$(2x')^2 + (2y')^2 + (2z')^2 = 2(2x')(2y')(2z')$$

i.e.

$$x'^2 + y'^2 + z'^2 = 4x'y'z'.$$

As the right-hand side is still congruent to 0 modulo 4, x', y' and z' are all even (this by the first part again). Writing $x' = 2x''$, etc., we now obtain

$$x''^2 + y''^2 + z''^2 = 8x''y''z''$$

and yet again x'', y'' and z'' are all even. We could continue forever in this way, halving the x, y and z values and yet retaining even, positive integers; for from

$$x_0^2 + y_0^2 + z_0^2 = 2^r x_0 y_0 z_0 \qquad (r \geqslant 1)$$

we have

$$\left(\frac{x_0}{2}\right)^2 + \left(\frac{y_0}{2}\right)^2 + \left(\frac{z_0}{2}\right)^2 = 2^{r+1}\left(\frac{x_0}{2}\right)\left(\frac{y_0}{2}\right)\left(\frac{z_0}{2}\right)$$

with $\frac{x_0}{2}, \frac{y_0}{2}$ and $\frac{z_0}{2}$ even. Hence, by the method of infinite descent, the Diophantine equation has no solutions. ■

SOLUTION TO SAQ 12 In looking for solutions of $x^4 - y^4 = 2z^2$, we may assume, without loss of generality, that $\gcd(x, y) = 1$; for, if $\gcd(x, y) = d > 1$, then putting $x = dx_1$, $y = dy_1$ and $z = d^2 z_1$ (since the equation shows that $d^2|z$) gives $x_1^4 - y_1^4 = 2z_1^2$, where $\gcd(x_1, y_1) = 1$.

As $x^4 - y^4$ is even and $\gcd(x, y) = 1$ it follows that x and y are both odd, and in consequence that $x^2 + y^2$, $x + y$ and $x - y$ are all even. So $x^2 + y^2 = 2r$, $x + y = 2s$ and $x - y = 2t$, for some integers r, s and t. Now

$$x^4 - y^4 = (x^2 + y^2)(x + y)(x - y) = 8rst = 2z^2,$$

and so $rst = \left(\frac{z}{2}\right)^2$.

Suppose for the moment that r, s and t are pairwise relatively prime. Then Lemma 2 (**B** page 244) tells us that r, s and t are each squares, so that $x^2 + y^2 = 2a^2$, $x + y = 2b^2$ and $x - y = 2c^2$ for some positive integers a, b and c. From this we have

$$4b^4 + 4c^4 = (x + y)^2 + (x - y)^2 = 2x^2 + 2y^2 = 4a^2.$$

But the equation $b^4 + c^4 = a^2$ is known to have no positive solutions (Theorem 11-3), contradicting the existence of such integers x and y.

To tidy up the loose ends we must finally confirm that

$$\gcd(s, t) = \gcd(r, s) = \gcd(r, t) = 1.$$

If $d|s$ and $d|t$ then $d|s \pm t$. That is, $d|x$ and $d|y$. But $\gcd(x, y) = 1$, and so $d|1$. Therefore $\gcd(s, t) = 1$.

If $p|r$ and $p|t$ (where p is prime), then $p|r - 2t^2$. That is, $p|xy$ and so by Euclid's Lemma $p|x$ or $p|y$. But $p|x - y\,(=2t)$, and so $p|x$ and $p|y$, which contradicts $\gcd(x, y) = 1$.

Similarly, if $p|r$ and $p|s$ then $p|2s^2 - r$. That is $p|xy$, which as above leads to a contradiction of $\gcd(x, y) = 1$. ■

8.4 Sums of Squares

Chapter 12 of **B** is devoted to the problem of representing integers as sums of squares. The culmination of the chapter is a theorem, due to Lagrange, which proves that every positive integer can be expressed as a sum of squares of four integers; in other words, the Diophantine equation

$$N = w^2 + x^2 + y^2 + z^2$$

has solutions for every positive integer N.

Since we allow the variable to take value zero, we have, as an immediate Corollary of Lagrange's Theorem, that every positive integer can be expressed as a sum of n squares, for each $n \geq 4$. So, in addition to the above result, there are just two interesting cases: which integers can be expressed as a sum of two squares, and which as a sum of three squares? In this section we shall give most of our attention to the first of these problems, which amounts to finding those integers N for which the Diophantine equation

$$N = x^2 + y^2$$

is solvable. Thereafter we shall sketch a proof of Lagrange's Theorem, and take a brief look at the three squares problem.

READ B Chapter 12, page 260 as far as page 263, line 8.

SAQ 13 Use the Lemma to express 4420 as a sum of two squares.

SOLUTION TO SAQ 13

$$4420 = 2^2 \cdot 5 \cdot 13 \cdot 17 = (2^2 + 0^2)(2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2).$$

Using the formula on the final line of page 262 of **B** three times:

$$\begin{aligned} 4420 &= (4^2 + 2^2)(3^2 + 2^2)(4^2 + 1^2) \\ &= (16^2 + 2^2)(4^2 + 1^2) \\ &= 66^2 + 8^2. \end{aligned}$$

COMMENT The answer is not unique. Indeed, in addition to the above,

$$4420 = 64^2 + 18^2 = 62^2 + 24^2 = 48^2 + 46^2.$$

We obtain the other solutions by changing the order of the bracketed terms, or by changing the order of the two squares within the brackets. For example, from the final line of the above solution,

$$4420 = (16^2 + 2^2)(1^2 + 4^2) = 24^2 + 62^2. \quad \blacksquare$$

To investigate whether or not the integer N is a sum of two squares, the Lemma suggests that we should look at its prime factorization. If each prime divisor of N is a sum of two squares then so too is N itself. Now primes come in 3 types:

(i) the even prime, $2 = 1^2 + 1^2$, is a sum of two squares;

(ii) odd primes of the form $4k + 3$, which, as we have seen in Theorem 12-1, cannot be expressed as a sum of two squares;

(iii) odd primes of the form $4k + 1$.

We shall now prove that all primes of type (iii) are sums of two squares, and having done this it will be a simple matter to complete the two squares problem. We are going to give an alternative proof to the one in **B**, our proof being essentially **B**'s proof of Lagrange's Theorem—the details are different, of course, but the methods are identical. Once you have sorted out the proof given below you should have no difficulty with **B**'s proof of Lagrange's Theorem (which we have left as optional reading).

The proof uses Fermat's descent method, but in a different way from our previous applications.

THEOREM (Fermat)

If $p \equiv 1 \pmod 4$ then p can be represented as a sum of two squares.

Preamble to the proof

We start by assuming that some multiple of p can be represented as a sum of two squares. More precisely, we assume that

$$mp = x^2 + y^2 \tag{1}$$

has a solution for some $1 < m < p$. From this we deduce that a smaller multiple of p can be so represented:

$$m'p = u^2 + v^2$$

where $1 \leq m' < m$. This is our customary descent step.

The difference is that this time we shall show that (1) does have a solution. The descent step tells us that there is then a smaller solution, and from this a smaller one, and so on. The process cannot go on for ever, and the only way it can terminate is by descending to a solution with $m' = 1$ (so that the descent step cannot be applied again). The inescapable conclusion is that $p = x^2 + y^2$ has a solution.

And now for the details.

PROOF *Part* (*i*) (The descent step)
Suppose that the equation $mp = x^2 + y^2$ has a solution in which $1 < m < p$. Let u and v be the least absolute residues modulo m of x and y, respectively. That is,

$$u \equiv x \pmod{m}, \quad v \equiv y \pmod{m}; \quad -\tfrac{1}{2}m < u,\ v \leq \tfrac{1}{2}m.$$

Then

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod{m},$$

and so

$$u^2 + v^2 = mr \quad (\text{for some } r \geq 0).$$

Now if $r = 0$, then $u = v = 0$ implying that $m|x$ and $m|y$. But then, from $mp = x^2 + y^2$, we conclude that $m|p$—which is a contradiction. So,

$$0 < r = \frac{1}{m}\{u^2 + v^2\} \leq \frac{1}{m}\left\{\frac{m^2}{4} + \frac{m^2}{4}\right\} < m.$$

Multiplying together the equations $mp = x^2 + y^2$ and $mr = u^2 + v^2$ gives

$$m^2rp = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

Now

$$xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{m}, \quad \text{implying that } m|xu + yv,$$

and

$$xv - yu \equiv xy - xy \equiv 0 \pmod{m}, \quad \text{implying that } m|xv - yu.$$

Putting $xu + yv = mX$ and $xv - yu = mY$ gives

$$m^2rp = m^2X^2 + m^2Y^2$$

or $rp = X^2 + Y^2$, where $1 \leq r < m$.

Part (*ii*) (To show $mp = x^2 + y^2$ has a solution with $1 \leq m < p$)
Since -1 is a quadratic residue of p (Corollary, **B** page 193), the equation $x^2 + 1 \equiv 0 \pmod{p}$ has a solution z. Selecting the least positive residue, we may assume that $0 < z \leq p - 1$. So there is an integer $m \geq 1$ such that

$$mp = z^2 + 1^2$$

and

$$m = \frac{1}{p}\{z^2 + 1^2\} \leq \frac{1}{p}\{(p-1)^2 + 1\} \leq \frac{1}{p}\{p^2 - 2(p-1)\} < p.$$

So there is a solution $(1 \leq m < p)$ to $mp = x^2 + y^2$ and hence, by part (i), a solution to $x^2 + y^2 = p$ for $p \equiv 1 \pmod{4}$. ■

SAQ 14 Given that $60^2 + 1^2 = 13 \cdot 277$, retrace the proof of the descent step to express the prime 277 as a sum of two squares.

SOLUTION TO SAQ 14 From

$$60^2 + 1^2 = 13 \cdot 277, \tag{1}$$

we have $m = 13$, $x = 60$ and $y = 1$. So $u \equiv 60 \pmod{13}$ and $v \equiv 1 \pmod{13}$ with $-7 < u, v < 7$, giving $u = -5$ and $v = 1$. Therefore

$$(-5)^2 + 1^2 = 2 \cdot 13 \tag{2}$$

so that $r = 2$. Multiplying equations (1) and (2) together,

$$\begin{aligned} 2 \cdot 13^2 \cdot 277 &= (60^2 + 1^2)((-5)^2 + 1^2) \\ &= (-299)^2 + 65^2, \end{aligned}$$

and on dividing both sides by 13^2 (and discarding the minus sign inside the square),

$$2 \cdot 277 = 23^2 + 5^2,$$

completing the first descent step.

Repeating with $m = 2$, $x = 23$ and $y = 5$ we have $u = v = 1$ and from

$$u^2 + v^2 = 1^2 + 1^2 = 1 \cdot 2,$$

$r = 1$. Multiplying the two equations,

$$2^2 \cdot 277 = (23^2 + 5^2)(1^2 + 1^2) = 28^2 + 18^2,$$

and on dividing both sides by 2^2,

$$277 = 14^2 + 9^2. \quad \blacksquare$$

After working through SAQ 14 you may feel that there ought to be an easier way of expressing an integer (like 277) as a sum of two squares. Indeed, you would be justified in thinking that a 'trial and error' method would get you to the solution more easily. Knowing that 277 can be expressed as a sum of two squares, we need only check $277 - 1^2$, $277 - 2^2, \ldots$, etc. until we find a square, in the knowledge that one must turn up by the time we reach $277 - 12^2$ (since $12^2 > \frac{277}{2}$).

Knowing that a prime of the form $p = 4k + 1$ can be represented as $x^2 + y^2$, mathematicians understandably turned to the task of finding ways of constructing the integers x and y in terms of p. Several such constructions emerged, but none of them particularly easy to employ. The first, due to Legendre, showed how to obtain x and y from the continued fraction of $\sqrt{p}$. The disadvantage of this method is that we first have to find the continued fraction of $\sqrt{p}$, which is no mean task when p is large. The next, due to Gauss, is easy to state:

> If $p = 4k + 1$, then $x \equiv \dfrac{(2k)!}{2(k!)^2} \pmod{p}$ and $y \equiv (2k)!\,x \pmod{p}$,
>
> where x and y are least absolute residues modulo p, satisfy $x^2 + y^2 = p$.

This is very neat, but try using it to express 277 ($k = 69$) as a sum of two squares!

For practical purposes, undoubtedly the best method for representing an integer as a sum of two squares is to resort to the suggested trial and error method, coupling it, of course, with the construction given in the Lemma at the foot of **B** page 262.

SAQ 15 Express $5321 = 17 \cdot 313$ as a sum of two squares.

SOLUTION TO SAQ 15 Testing $313 - 1^2, 313 - 2^2, \ldots$ for being a square, we eventually find that $313 - 12^2 = 13^2$. Therefore $313 = 12^2 + 13^2$ and

$$5321 = (4^2 + 1^2)(12^2 + 13^2) = 61^2 + 40^2.$$

Had we written $5321 = (4^2 + 1^2)(13^2 + 12^2)$, the formula for this product at the foot of **B** page 262 gives the alternative answer

$$5321 = 64^2 + 35^2.$$

These two are the only solutions in non-negative integers. ■

We have seen that some integers can be represented in more than one way as a sum of two squares. This is not true of primes. A prime of the form $4k + 1$ is representable in a unique way as a sum of two squares of positive integers.

READ B page 265, from line 7 to the foot of the page.

NOTE *Page 265, line 12*
The conclusion of this line is justified by

$$a^2d^2 - b^2c^2 = (a^2 + b^2)d^2 - (c^2 + d^2)b^2 = pd^2 - pb^2. \quad \blacktriangle$$

Having solved the problem of which primes are sums of two squares we are now ready to determine which integers are sums of two squares.

READ B from page 267, line 7 to page 269, line 15.

SAQ 16 Which years in this decade (1980–1989) can be represented as a sum of two squares? For each affirmative answer find one such representation.

SAQ 17 **B** page 271, Problems 12.2, number 3 parts (a), (b), (c) and (d).

SAQ 18 Show that if $p = 4k + 1$ is prime, then $2p = x^2 + y^2$ has exactly one solution with $0 < y < x$.

SAQ 19 For which integers n $(0 \leq n \leq 35)$ is the congruence

$$x^2 + y^2 \equiv n \pmod{36}$$

not solvable? Hence show that at least 40 per cent of the positive integers $\leq 10^6$ are not expressible as a sum of two squares.

SOLUTION TO SAQ 16

$1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$

$1981 = 7 \cdot 283$

$1982 = 2 \cdot 991$

$1983 = 3 \cdot 661$

$1984 = 2^6 \cdot 31$

$1985 = 5 \cdot 397$

$1986 = 2 \cdot 3 \cdot 331$

$1987 =$ prime

$1988 = 2^2 \cdot 7 \cdot 71$

$1989 = 3^2 \cdot 13 \cdot 17$

Excluding 1985 and 1989, each of the remaining years is divisible by a prime $p = 4k + 3$ but not divisible by p^2. By Theorem 12-3, these years are not representable as sums of two squares.

$$1985 = 32^2 + 31^2 = 44^2 + 7^2,$$

$$1989 = 33^2 + 30^2 = 42^2 + 15^2. \quad \blacksquare$$

SOLUTION TO SAQ 17

(a) Since 2^n is not divisible by any odd prime, the result follows from Theorem 12-3. More specifically:

$$n \text{ even} \implies 2^n = (2^{n/2})^2 + 0^2,$$
$$n \text{ odd} \implies 2^n = (2^{(n-1)/2})^2 + (2^{(n-1)/2})^2.$$

(b) Modulo 9, the squares are 0, 1, 4 or 7. So for any two integers x and y,

$$\begin{aligned} x^2 + y^2 &\equiv \{0, 1, 4, 7\} + \{0, 1, 4, 7\} \\ &\equiv 0, 1, 2, 4, 5, 7 \text{ or } 8 \pmod 9. \end{aligned}$$

Therefore $n \equiv 3, 6 \pmod 9$ cannot be represented as the sum of two squares.

(c) If $n = \dfrac{r(r+1)}{2} + \dfrac{s(s+1)}{2}$ then

$$4n + 1 = 2r(r+1) + 2s(s+1) + 1 = (r+s+1)^2 + (r-s)^2.$$

(d) $F_n = (2^{2^{n-1}})^2 + 1^2$, for $n \geq 1$. ■

SOLUTION TO SAQ 18

If $2p = x^2 + y^2$, then $x^2 + y^2 \equiv 2 \pmod 4$, which means that x and y are both odd. In that case

$$x^2 + y^2 = 2\left(\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2\right),$$

so that $p = \left(\dfrac{x+y}{2}\right)^2 + \left(\dfrac{x-y}{2}\right)^2$. But we know that p can be represented as a sum of two (positive) squares in a unique way, and so $\dfrac{x+y}{2}$ and $\dfrac{x-y}{2}$ (and in consequence x and y) are uniquely determined. ■

SOLUTION TO SAQ 19

$x^2 + y^2 \equiv n \pmod{36}$ has solutions if and only if each of $x^2 + y^2 \equiv n \pmod 4$ and $x^2 + y^2 \equiv n \pmod 9$ have solutions. We saw in SAQ 17(b) that $x^2 + y^2 \equiv n \pmod 9$ has solutions except for $n = 3$ and 6. Similarly, $x^2 + y^2 \equiv n \pmod 4$ has solutions for $n = 0$, 1 and 2 but not for $n = 3$. It follows that $x^2 + y^2 \equiv n \pmod{36}$ has solutions for all but the following fifteen values of n:

$$n = 3, 6, 7, 11, 12, 15, 19, 21, 23, 24, 27, 30, 31, 33, \text{ and } 35.$$

Consequently, in each set of 36 consecutive integers there are at least 15 which are not sums of two squares. (Note that if n is congruent modulo 36 to a sum of two squares, it does not follow that n itself is a sum of two squares. For example, 38 is not a sum of two squares, but $38 \equiv 1^2 + 1^2 \pmod{36}$.) Therefore the percentage of positive integers not exceeding 10^6 which are not sums of two squares is at least

$$\frac{\frac{15}{36} \cdot 10^6 - 36}{10^6} \cdot 100 \simeq 41.7 > 40.$$

(Note that since 36 does not divide 10^6 exactly, we subtract 36 in the numerator to play safe.) ■

To round off the section we shall take a brief look at the three squares and four squares problems.

As commented earlier, the proof in **B** of Lagrange's Theorem, that every positive integer is a sum of four squares, is remarkably similar to the proof we have given for the two squares problem. It hinges around an identity (Lemma 1, **B** page 275) showing that if two integers are each representable as a sum of four squares then so too is their product. This suggests that we attack the problem by establishing that every prime is a sum of four squares. The even prime $2 = 1^2 + 1^2 + 0^2 + 0^2$ creates no problem. The proof for the odd primes uses the descent method in just the same way as in the case of two squares.

For any odd prime p, we assume that

$$mp = w^2 + x^2 + y^2 + z^2$$

has a solution for some m such that $1 < m < p$. We achieve the descent step by deducing from this that

$$m'p = s^2 + t^2 + u^2 + v^2$$

for some smaller multiple m' such that $1 \leq m' < m$. The second part of the proof shows that the initial assumption, that an appropriate multiple of p can be expressed as a sum of four squares, is valid. (This is Lemma 2, **B** page 275.)

The three squares problem is much more difficult, simply because it is not true that if two integers are each the sum of three squares then so too is their product. For instance, $3 = 1^2 + 1^2 + 1^2$ and $5 = 2^2 + 1^2 + 0^2$, but their product, 15, is not a sum of three squares. This forces a completely different approach to the problem.

Discovering which integers cannot be represented as a sum of three squares is an easy matter; the difficulty comes when one tries to prove that these are the only such integers.

READ B Section 12.3, page 273 as far as page 274, line −3.

SAQ 20 Determine whether or not each of the following integers can be represented as a sum of two squares and/or three squares.

(a) 1,000,003 (prime), (b) 10!, (c) 100! (Hint: Use Theorem 6-9, **B** page 126).

SOLUTION TO SAQ 20

(a) $1{,}000{,}003 \equiv 3 \pmod 4$, so it is not a sum of two squares.

$1{,}000{,}003 \equiv 3 \pmod 8$, so it is a sum of three squares.

(b) $10! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$. Since $7 | 10!$ but $7^2 \nmid 10!$, $10!$ is not a sum of two squares.

Writing $10! = 4^4 \cdot (3^4 \cdot 5^2 \cdot 7)$, and discovering that $3^4 \cdot 5^2 \cdot 7 \equiv 7 \pmod 8$ (which is easily seen since $3^2 \equiv 5^2 \equiv 1 \pmod 8$), we have that $10!$ is of the form $4^4(8m + 7)$ and so, by Theorem 12-5, is not a sum of three squares.

(c) Since $100!$ is divisible by several primes $p = 4k + 3$ but not by their squares (e.g. $p = 59$), it follows that $100!$ is not a sum of two squares.

Using Theorem 6-9 (**B** page 126), the exponent of the highest power of 2 dividing $100!$ is

$$\left[\frac{100}{2}\right] + \left[\frac{100}{4}\right] + \left[\frac{100}{8}\right] + \left[\frac{100}{16}\right] + \left[\frac{100}{32}\right] + \left[\frac{100}{64}\right]$$

$$= 50 + 25 + 12 + 6 + 3 + 1 = 97.$$

Therefore $100! = 2^{97} m = 4^{48}(2m)$, where m is odd. As this is not of the form $4^n(8m + 7)$, $100!$ is a sum of three squares. ■

8.5 Summary

The study of Diophantine problems is a vast subject lying at the heart of number theory. In this unit we have looked at a selection of historically significant Diophantine equations.

Section 8.1 investigated Pell's Equation, $x^2 - dy^2 = 1$, and the closely related equation $x^2 - dy^2 = -1$, where $d \geq 2$ is a non-square integer. We discovered that all solutions of these equations are readily obtained from the convergents of the continued fraction of $\sqrt{d}$.

In Section 8.2, we focussed on the equation associated with Pythagoras' Theorem, $x^2 + y^2 = z^2$. The geometric interpretation of the corresponding Diophantine problem is to find all right-angled triangles with sides of integer length. Appreciating that all positive solutions arise as scalar multiples of primitive ones, i.e. ones in which $\gcd(x, y, z) = 1$, we successfully classified all primitive Pythagorean triples.

Section 8.3 centred around Fermat's Last Theorem, the unresolved conjecture that $x^n + y^n = z^n$ has no non-trivial solutions for $n \geq 3$. Using our result on the Pythagorean equation, we proved Fermat's Last Theorem for the particular case $n = 4$. The strategy of the proof incorporated Fermat's method of infinite descent, for which we subsequently found several other applications.

Section 8.4 turned to the problem of representing integers as sums of squares. We concentrated on the two squares problem, classifying those integers N for which the Diophantine equation $N = x^2 + y^2$ has solutions. We observed that Lagrange's Theorem, which states that every positive integer is a sum of four squares, can be proved in a very similar manner to the two squares problem, and we outlined that proof. Finally, we discovered that no integer of the form $4^k(8m + 7)$ can be expressed as a sum of three squares. We omitted the (difficult) proof that all other positive integers are sums of three squares.

The main definitions and results encountered in this unit are listed in the corresponding entry in the Handbook.

0 335 14011 4

Elementary Number Theory

Second Edition

David M. Burton